



Cybersecurity Assistance for Nonprofits

Security Feature Matrix CRM Vendor Comparison

Give Butter
Little Green Light

First Edition

October 2026

As the 501Secure program enters its third year, our expert volunteers continue to serve the nonprofit community with practical cybersecurity information, awareness programming, expert guidance, and free services.

We hope you find this Security Feature Matrix helpful when evaluating cloud software subscriptions and vendors.



Cybersecurity Assistance for Nonprofits

Questions about this guide or the 501Secure program contact the 501Secure Team at info@501Secure.org.

For immediate cybersecurity assistance, email help@501Secure.org.

Security Feature Matrix

CRM Vendor Comparison

Give Butter and Little Green Light

Give Butter

Consider: Does upgrading provide security or administrative capabilities that address an identified organizational risk, or does it primarily add fundraising and operational features? Before paying for a higher tier, determine whether the additional capabilities improve protection of member and donor information, account access, or administrative oversight enough to justify the additional cost.

Control	Availability / Plan	Control's Purpose/benefits	Compensatory Method	Control Mapping	Documentation Link
IAM	Standard, Plus	User accounts can be added, managed, and removed while controlling access to the organization's Givebutter account. This would help the client control which board members or volunteers can access fundraising and donor information.	Review board member and volunteer accounts quarterly, immediately remove former members or volunteers, and verify that only authorized users have access to member information and donation records.	PR.AA-01	Manage account users
Conditional Access	Not Available	Controls access based on conditions such as a user's device, location, or IP address. This could provide additional protection when board members access fundraising information remotely or from personal devices.	Require MFA and strong passwords.	PR.AA-05	Not documented by the vendor
RBAC	Standard, Plus	Limits what users can view or manage based on their assigned role. This would help the client prevent board members or volunteers from receiving unnecessary access to donor and fundraising information.	Follow least privilege when assigning roles.	PR.AA-05	Manage account users
Single Sign-on	Not Available	Limits what users can view or manage based on their assigned role. This would help the client prevent board members or volunteers from receiving unnecessary access to donor and fundraising information.	Use unique passwords and MFA.	PR.AA-03	Not documented by the vendor

Global MFA	Standard, Plus	Givebutter requires 2FA for additional login security and can require verification when users sign in from a new location. This would help reduce the client's risk of another account takeover involving fundraising or donor information.	Require all staff to enable MFA.	PR.AA-03	Keeping Givebutter account secure Troubleshooting sign-in issues
Admin MFA Audit	Standard, Plus	Allows administrators to determine whether users have MFA enabled. This would help the client identify board members or volunteers whose accounts may need stronger protection.	Periodically review user security settings.	PR.AA-05	Manage account users
MFA Options	Standard, Plus	Provides additional ways to verify a user's identity beyond a password. This can better protect fundraising and donor information if a user's password is compromised.	Encourage every user to enable 2FA.	PR.AA-03	Mobile app & verification
MFA Recovery	Standard, Plus	Provides a way for legitimate users to regain access when their normal MFA method is unavailable. This helps restore access without permanently weakening account security.	Verify identity before resetting 2FA.	PR.AA-01	Manage personal profile
Session Limiting / Timeout	Standard, Plus	Limits how long an authenticated session remains active. This can reduce unauthorized access if Givebutter is left signed in on a board member's personal device.	Require board members to sign out of Givebutter after each session when using personal devices and enable MFA on every account.	PR.AA-03	Session timeout
Token Duration	Not Available	Controls how long authentication remains valid before another login or verification is required. This could reduce how long compromised authentication remains useful to an unauthorized person.	Require MFA and strong password policies to reduce the risk of stolen sessions.	PR.AA-04	Not documented by the vendor
Risk-Based Conditional Access	Not Available	Evaluates login circumstances and applies additional access requirements when an attempt appears risky. This could help protect the client's fundraising account from suspicious login attempts.	Require MFA for all users and regularly review account access.	PR.AA-05	Not documented by the vendor
Suspend All Sessions	Standard, Plus	Allows users to end active login sessions when they believe their account may be compromised. This could help the client quickly remove unauthorized	If a board member suspects their account has been compromised, immediately reset	PR.AA-04	Manage personal profile

		access after another suspected account takeover.	the password, remove access if necessary, and verify MFA before restoring access.		
Device, Location, IP Information	Standard, Plus	Allows users to review active login sessions and identify sessions they do not recognize. This could help the client identify suspicious access to fundraising or donor information.	Review account activity regularly and enable MFA.	DE.CM-03	Active session information
Forced Password Reset	Not Available	Requires a password to be changed when credentials may have been compromised. This could help secure a board member or volunteer's Givebutter account after suspicious activity.	Remove or restrict the user's account access and require the user to reset their password and verify 2FA before restoring access.	PR.AA-03	Reset Password (partial documentation)
Availability of Logs	Standard, Plus	Provides records of account activity that can be reviewed after suspicious activity or changes occur. This could help the client understand what happened during a security incident involving its fundraising system.	Perform periodic account reviews and maintain administrative records.	DE.CM-03	Not documented by the vendor
Token Configuration Across Devices/IPs	Not Available	Controls whether authenticated access can continue when a device, location, or IP address changes. This could reduce the ability to reuse stolen authentication from another device or location.	Use MFA and remove user access when accounts are no longer needed.	PR.AA-04	Not documented by the vendor
SIEM / CASB Integration	Not Available	Connects Givebutter security information with external monitoring tools. This could provide centralized security monitoring, although it may be more advanced than this client's immediate needs.	Export available data manually and monitor accounts through organizational security processes.	DE.CM-01	Not documented by the vendor
API Integration for User Provisioning / Deprovisioning	Not Available	Would automate adding and removing user accounts instead of requiring an administrator to manage each account manually. This could reduce administrative work and help prevent former board members or volunteers from retaining access.	Administrators should manually invite users, assign only necessary roles, regularly review account access, and immediately remove users who no longer require access.	PR.AA-01	Manage Account Users Public API Keys

Is This Tier Worth It?

Givebutter Standard	Givebutter Plus
Highly worth it: Best value because it provides the core fundraising and CRM capabilities without a monthly subscription. It can help the organization move member and donor information out of a shared Word document and into a centralized system. Before using it, the organization should require MFA, assign access based on job responsibilities, use organizational Google Workspace emails, and confirm who is responsible for maintaining the records.	Moderately worth it: Worth considering if the organization needs advanced workflows, automation, bulk communication, or accounting integrations. However, Plus does not appear to add the advanced identity controls that would most directly address the client's previous account takeover. The organization should upgrade only after establishing MFA, account-removal procedures, least-privilege access, secure PayPal processes, and a clear need for the additional operational features.

Little Green Light

Consideration: Little Green Light provides all features and unlimited users with every account, so organizations do not have to purchase a higher security tier to access additional controls. Pricing increases based on the number of constituent records rather than security features. Consider whether the organization's number of member and donor records justifies the monthly cost and whether LGL's available security controls are sufficient for the sensitivity of the information being stored.

Control	Availability / Plan	Control's Purpose/benefits	Compensatory Method	Control Mapping	Documentation Link
IAM	All Plans Available in: Plan 1, Plan 2, Plan 3, Plan 4, Plan 5, Plan 6, Plan 7, Plan 8	User accounts can be centrally added, updated, deactivated, and assigned individual access. This would help the client move member information out of a shared Word document while controlling which board members or volunteers can access the CRM.	Review board member and volunteer accounts quarterly, immediately deactivate former members, and require every user to have an individual organizational email account.	PR.AA-01	Manage team members
Conditional Access	Not Available	Controls access based on conditions such as a user's device, location, or IP address. This could provide additional protection when board members access member information remotely or from personal devices.	Require organization-wide MFA, use organizational Google Workspace accounts, enable geographic login alerts, and prohibit access from public or unmanaged computers.	PR.AA-05	Not documented by the vendor
RBAC	All Plans Available in: Plan 1, Plan 2, Plan 3, Plan 4, Plan 5, Plan 6, Plan 7, Plan 8	Limits what users can view or change based on their assigned responsibilities. This would allow the client to give board members and volunteers only the access they need to member and donor information.	Follow least privilege by assigning users the lowest role needed for their responsibilities and reviewing role assignments quarterly.	PR.AA-05	Team member/user roles and permissions
Single Sign-on	Not Available	Allows users to access the CRM through a centrally managed organizational identity. This could simplify access for board members and reduce the number of separate passwords they need to manage.	Require users to register with their individual organizational Google Workspace email, use a unique password, and enable MFA.	PR.AA-03	Not documented by the vendor
Global MFA	All Plans Available in: Plan 1, Plan 2, Plan 3, Plan 4, Plan 5, Plan 6, Plan 7, Plan 8	Allows an administrator to require MFA instead of relying on individual users to enable it themselves. This would help reduce the client's risk of another account takeover after member information is moved into the CRM.	Enable the account-wide "Require 2-step verification" setting before member and donation information is moved into the CRM.	PR.AA-03	Enable and manage 2-step verification
Admin MFA Audit	Not Available	Allows administrators to determine which users	Turn on account-wide MFA so every user is required to	PR.AA-05	Not documented

		have MFA enabled. This would help the client identify board members or volunteers whose accounts are not adequately protected.	use it rather than relying on administrators to review voluntary enrollment.		by the vendor
MFA Options	All Plans Available in: Plan 1, Plan 2, Plan 3, Plan 4, Plan 5, Plan 6, Plan 7, Plan 8	Provides additional methods for verifying a user's identity beyond a password. This can better protect member and donor information if a user's password is compromised.	Require board members to use an Authenticator application instead of email verification whenever possible.	PR.AA-03	MFA options
MFA Recovery	All Plans Available in: Plan 1, Plan 2, Plan 3, Plan 4, Plan 5, Plan 6, Plan 7, Plan 8	Provides a secure way for legitimate users to regain access when their normal MFA method is unavailable. This helps prevent users from bypassing security controls simply because they lose access to an authentication method.	Require users to generate recovery codes and store them in an approved password manager rather than on personal devices or in unsecured documents.	PR.AA-01	MFA Recovery
Session Limiting / Timeout	All Plans Available in: Plan 1, Plan 2, Plan 3, Plan 4, Plan 5, Plan 6, Plan 7, Plan 8	Automatically ends a user's session after a set period of inactivity. This can reduce unauthorized access if a board member leaves member information open on a personal device.	Set the organization-wide timeout to 15 or 30 minutes and require users to manually sign out after completing their work.	PR.AA-03	Automatically log out users who are idle
Token Duration	Not Available	Controls how long authentication remains valid before additional verification is required. This can reduce how long compromised authentication remains useful to an unauthorized person.	Use the shorter MFA reverification period and combine it with a 15- or 30-minute idle timeout.	PR.AA-04	Not documented by the vendor
Risk-Based Conditional Access	Not Available	Evaluates login circumstances and applies stronger requirements when access appears risky. This could provide additional protection against suspicious attempts to access the client's member information.	Enable account-wide MFA, short session timeouts, geographic login alerts, and immediate password changes when suspicious activity is reported.	PR.AA-05	Not documented by the vendor
Suspend All Sessions	Not Available	Allows active login sessions to be ended when an account may have been compromised. This could help the client quickly remove unauthorized access to member or donor information after a suspected account takeover.	Immediately deactivate the affected user, reset the password, review the associated email account, and restore access only after MFA has been secured.	PR.AA-04	Not documented by the vendor
Device, Location, IP Information	All Plans Available in: Plan 1, Plan 2, Plan	Provides information about where and how accounts are being accessed. This could help	Require each board member to enable login alerts and immediately report any alert they do not recognize.	DE.CM-03	Enable alerts for logins from new

	3, Plan 4, Plan 5, Plan 6, Plan 7, Plan 8	the client identify unfamiliar access to member information, especially when board members use personal devices.			geographical locations
Forced Password Reset	Not Available	Requires credentials to be changed when a password may have been compromised. This could help secure access to member information following suspicious account activity.	Deactivate the compromised user until the user resets the password, secures their organizational email, and confirms MFA enrollment.	PR.AA-03	Best practices: Data security and using Little Green Light
Availability of Logs	All Plans Available in: Plan 1, Plan 2, Plan 3, Plan 4, Plan 5, Plan 6, Plan 7, Plan 8	Maintains activity and user attribution within CRM records, which can provide accountability for changes made in the system. This could help the client determine who accessed or changed member and donor information.	Maintain a separate access-review record, document Administrator changes, review unusual member-record changes, and retain financial records outside the CRM when legally required.	DE.CM-03	Manage team members
Token Configuration Across Devices/IPs	Not Available	Controls whether authenticated access can continue across different devices, locations, or IP addresses. This could reduce unauthorized reuse of authentication when member information is accessed remotely.	Require MFA, enable geographic alerts, use short session timeouts, and limit CRM access to supported and updated personal devices.	PR.AA-04	Not documented by the vendor
SIEM / CASB Integration	Not Available	Connects CRM security information with external security monitoring tools. This could improve centralized monitoring, although it may be more advanced than the client's immediate security needs.	Maintain manual security incident records, review account access periodically, and use Google Workspace security reporting for organizational email activity.	DE.CM-01	Not documented by the vendor
API Integration for User Provisioning / Deprovisioning	Not Available	Would automate adding and removing user access when board members, volunteers, or staff change. This could reduce manual work and help ensure former users do not retain access to member information.	Administrators should manually add individual users, assign the appropriate role, regularly review the Team Members list, and immediately deactivate users who no longer need access.	PR.AA-01	Not documented by the vendor

Is This Tier Worth It?

Because all Little Green Light accounts include the same features, this section should evaluate the pricing tiers, not different security packages.

Plan 1: 2500	Plan 2: 5000	Plan 3: 10000	Plans 4-8: 20000 or More
High: Best value for a small nonprofit moving member information from a Word document into a centrally managed CRM. Confirm that the organization has fewer than 2,500 member and donor records before selecting this tier.	High: Good for a growing organization that expects to store more than 2,500 constituent records. The upgrade increases storage capacity but does not provide additional security controls.	Medium: Worth considering only when the number of legitimate member and donor records requires the larger tier. Review and remove duplicates before upgrading.	Low-Medium: Appropriate for organizations with a large constituent database, but likely unnecessary for this client unless its membership and donor records are substantially larger than expected.