



CASE MANAGEMENT SYSTEM

Case Management System Privacy Policy

The Falls Gaming, LLC d/b/a Solvora Studios | Effective October 17, 2026

This policy explains how CMS, CMSO, and the official Case Management System Discord application process information, how information is shared and retained, and how users may make privacy or deletion requests.

Effective date: October 17, 2026

Last updated: October 24, 2026

This Privacy Policy explains how Case Management System and Case Management System Online, including the official Case Management System Discord application (collectively, the **Service**), process information. The Service is developed and licensed by **The Falls Gaming, LLC, doing business as Solvora Studios** (Solvora Studios, we, us, or our).

CMS and CMSO may be self-hosted, hosted for one organization, or connected to optional third-party services. The organization or Discord community that configures and operates a particular deployment (the **Community Operator**) controls the records and configuration within that deployment. This policy describes our general practices for the official application and our controlled services. A Community Operator may provide additional notices that apply to its deployment.

1 Scope

This policy applies when you:

- interact with the official Case Management System Discord application;
- sign in to or use a CMS or CMSO deployment controlled by us;
- submit a form, service request, ticket, report, record, evidence item, or other content through the Service; or
- contact us about support, privacy, security, or account administration.

For an independently operated or self-hosted deployment, the Community Operator is responsible for that deployment's collection, use, retention, disclosure, and deletion of information. Direct deployment-specific questions and requests to that Community Operator first.

2 Information We Process

The Service may process the following categories of information, depending on how a Community Operator configures it and which features you use.

2.1 Discord account and server information

- Discord user ID, username, display name, avatar, and related profile information;
- Discord server or guild ID, channel ID, role ID, role membership, permission information, and server configuration;
- interaction IDs, command names, form or modal responses, timestamps, and other information needed to process an interaction;
- message IDs, thread IDs, webhook information, and message content when a configured feature requires that content and Discord permits access; and
- authentication tokens, session identifiers, and OAuth authorization details needed to sign you in and connect the Service to Discord. Secret credentials are not intended to be displayed to other users.

2.2 Community and case management information

- forms, reports, tickets, service requests, applications, and responses;
- citizen or member profiles, display names, community-issued identifiers, roleplay identifiers, affiliations, and contact details entered by authorized users;
- case files, investigations, court or administrative records, offenses, notes, assignments, decisions, and audit history;
- evidence metadata, uploaded files, images, videos, links, serial numbers, vehicle plates, fingerprint identifiers, and related associations;
- configuration data, access-control rules, connected roles, channels, categories, integrations, and retention settings; and
- any other content that a user or Community Operator chooses to submit to the Service.

The Service is commonly used for gaming, simulation, roleplay, and community administration. Users should not enter real-world government identifiers, financial account information, medical information, passwords, or other legally protected or highly sensitive personal information unless the Community Operator has a lawful, documented reason and has configured appropriate safeguards.

2.3 Technical and security information

- IP address, browser and device information, operating system, request time, referring page, and diagnostic information;
- login, session, security-event, audit, rate-limit, and error logs;
- storage usage, feature usage, and performance information; and
- records needed to prevent abuse, investigate incidents, and maintain the Service.

2.4 Support and communications

We may process the content of support requests, reports, deletion requests, security notices, and other communications, together with the contact and account information needed to respond.

3 How We Obtain Information

We obtain information:

- directly from users and Community Operators;
- from Discord through its APIs and OAuth services;
- from optional integrations enabled by a Community Operator, such as file-hosting, cloud-document, media, or game-server services;
- automatically from the browser, server, and security logs; and
- from authorized administrators who create, update, link, or import records.

4 How We Use Information

We process information only as reasonably necessary to:

- authenticate users and apply role-based permissions;
- receive and respond to commands, interactions, forms, requests, and tickets;
- create, organize, search, link, display, audit, and retain authorized community records;
- provide evidence, record, workflow, notification, and document-generation features;
- send configured Discord messages, notifications, reminders, and status updates;
- operate, secure, troubleshoot, maintain, and improve the Service;
- enforce the Terms of Service, license terms, and Community Operator rules;
- investigate fraud, abuse, security incidents, and unauthorized access;
- comply with Discord's requirements and applicable law; and

- respond to user requests and legal process.

We do not sell Discord API data or personal information. We do not disclose Discord API data to data brokers or advertising networks, and we do not use message content obtained through Discord APIs to train machine-learning or artificial-intelligence models.

5 Legal Bases Where Applicable

Where privacy law requires a legal basis, processing may be based on:

- performance of a contract or steps requested before entering a contract;
- our legitimate interests or a Community Operator's legitimate interests in operating, securing, and administering the Service;
- consent, when consent is requested and may be withdrawn;
- compliance with a legal obligation; or
- protection of the rights, safety, and security of users, communities, the public, Discord, and the Service.

The applicable basis depends on the feature, deployment, jurisdiction, and relationship between the user and the Community Operator.

6 How Information Is Shared

Information may be disclosed only as described below and subject to applicable permissions and law.

6.1 Authorized community users

Records and content may be visible to Community Operators and to users assigned authorized roles. Visibility may depend on community membership, record type, classification, assignment, role, and other access controls. Community Operators are responsible for assigning permissions appropriately.

6.2 Service providers

We and Community Operators may use hosting, storage, database, security, communications, media, and support providers to operate the Service. These providers may process information only to provide their contracted services and subject to applicable confidentiality and data-protection obligations.

6.3 Optional integrations

If enabled, information may be exchanged with Discord, Google services, FiveManage, Wispybyte, game-server systems, or another integration selected by the Community Operator. Each third party processes information under its own terms and privacy policy. The Service does not enable every integration in every deployment.

6.4 Legal and safety disclosures

Information may be preserved or disclosed when reasonably necessary to comply with law, legal process, or a valid governmental request; protect rights or safety; investigate abuse or a security incident; enforce applicable terms; or establish, exercise, or defend legal claims.

6.5 Organizational changes

Information may be transferred as part of a merger, acquisition, financing, reorganization, bankruptcy, or sale of assets, subject to applicable law and continued protection of the information.

7 Data Retention

We retain information only for as long as reasonably necessary for the purposes described in this policy, to comply with law, to resolve disputes, and to enforce agreements. Retention varies by record type and deployment configuration.

- Discord API data is retained only while necessary for the Service's stated functionality or another lawful requirement.
- Session and authentication data generally remain only for the active session or configured session lifetime.
- Operational, security, and audit logs may be retained for a limited period needed for security, accountability, troubleshooting, and legal compliance.
- Community records remain according to the Community Operator's configured retention rules, administrative decisions, backup schedule, and legal obligations.
- Evidence media and files may have separate retention periods displayed within the Service.
- Backups may retain deleted information temporarily until the backup cycle expires.

Subject to applicable law, Discord API data will be updated or deleted when Discord or the affected user validly requests it, when it is no longer needed for approved functionality, or when operation of the relevant application ends.

8 Security

We use reasonable administrative, technical, and organizational safeguards designed to protect information from unauthorized access, alteration, disclosure, loss, or destruction. Safeguards may include access controls, role-based authorization, audit logs, credential protection, secure transport, encryption where supported, backups, and incident-response procedures.

No system is completely secure. Users and Community Operators must protect their credentials, restrict administrative access, install security updates, maintain secure hosting, and configure integrations responsibly. A self-hosted Community Operator is responsible for the security of its servers, databases, backups, domains, certificates, and administrator accounts.

9 Your Choices and Privacy Rights

Depending on applicable law, you may have rights to request access, correction, deletion, restriction, objection, portability, or withdrawal of consent. You may also have the right to complain to a privacy regulator.

To exercise a right or request deletion of Discord API data:

1. Contact the administrators of the Discord server or organization that operates the relevant CMSO deployment.
2. For the official Case Management System application or a deployment controlled by The Falls Gaming, LLC, use the support contact or support server linked from the application's official Discord profile or installation page and clearly label the request **Privacy Request**.
3. Include your Discord user ID, the affected community or server ID, the relevant record identifier if known, and the specific action requested. Do not send passwords, authentication tokens, or unnecessary sensitive information.

We or the Community Operator may need to verify your identity and authority before acting. A request may be limited or denied where retention is required by law, necessary to protect another person, needed for security or fraud prevention, or otherwise permitted by applicable law. When deletion of a complete record is not permitted, identifying information may be restricted, corrected, or de-identified where appropriate.

Removing the application from a Discord server or revoking OAuth access stops future access through that authorization but may not automatically delete records previously submitted to a separately operated CMSO deployment. Submit a deletion request to the relevant Community Operator for those records.

10 Children and Minimum Age

The Service is not directed to children under 13 or under the minimum age required to use Discord in their jurisdiction, whichever is higher. We do not knowingly collect Discord API data from a person who may not lawfully

use Discord. If you believe prohibited information has been submitted, contact the relevant Community Operator or the official support contact so it can be reviewed and deleted as appropriate.

11 International Processing

Information may be processed in the country where the Community Operator, hosting provider, or service provider operates. Where required, appropriate safeguards will be used for international transfers. Community Operators are responsible for determining whether their deployment requires additional transfer notices or agreements.

12 Third Party Services

Discord and other integrations are independent third parties. Their handling of information is governed by their own policies. Discord's current developer terms and policies are available at:

- [Discord Developer Terms of Service](#)
- [Discord Developer Policy](#)
- [Discord Privacy Policy](#)

13 Changes to This Policy

We may update this policy to reflect changes in the Service, law, security practices, or third-party requirements. The effective date above will be updated when changes take effect. Material changes may also be announced through the Service, the official support server, repository release notes, or another reasonable channel. Continued use after the effective date is subject to the updated policy where permitted by law.

14 Contact

For a community-controlled deployment, contact that community's administrators. For the official Case Management System Discord application or a service controlled by The Falls Gaming, LLC, use the support contact or support server published in the application's official Discord profile or installation page and label the message **Privacy Request**.

The Falls Gaming, LLC may require a Community Operator to handle a request when that operator independently controls the relevant records.