



IRONCLAD TOURNAMENTS

PRIVACY POLICY

IronClad Tournaments Privacy Notice

VERSION 1.3

EFFECTIVE

Effective date: 23 September 2026

Marco Stucchi, based in New South Wales, Australia, and Simone Vitiello, based in Italy, are the responsible operators of the Service.

ironclad.tournaments@gmail.com

Contents

1. Who is responsible for this Service	4
2. Scope	4
3. Information we process	4
4. Sources	7
5. Why we process information	8
6. Legal grounds where applicable	8
7. Authentication	8
8. Profiles, avatars and optional Discord	9
9. Steam and Relic verification	9
10. Registration and durable acceptance	9
11. Match results and private evidence	9
12. Dice and Polls	10
13. Notifications, email and Admin Assistance	10
14. Public information and Competition History	11
15. Providers and recipients	11
16. International processing	11
17. Cookies, session storage and tracking	12
18. Retention	13
19. Account closure and deletion	14
20. Privacy choices and rights	15
21. Rules-based processing and human review	16
22. Security and incidents	16
23. Age	16

24. External links and services	16
25. Changes and versions	16
26. Contact and complaints	17

PRIVACY CONTACT

Privacy requests and complaints may be sent to ironclad.tournaments@gmail.com.

1. Who is responsible for this Service

“IronClad Tournaments” is the project and operating name currently used by:

- Marco Stucchi, based in New South Wales, Australia; and
- Simone Vitiello, based in Italy.

Those two natural persons are the responsible operators of the Service and the people to contact about its handling of personal information. In this Policy, “IronClad”, “we”, “us” and “our” mean Marco Stucchi and Simone Vitiello only.

Admins are delegated operational personnel authorized to perform specified administration or support functions. Admins are not included in “IronClad”, “we”, “us” or “our”, do not become responsible operators merely because of their role, and may handle personal information only within their delegated authority and this Policy.

This wording does not represent IronClad Tournaments as a company, incorporated body, registered Australian business name, Australian partnership, ABN holder or other registered entity. It does not assign an unverified “joint controller” or other formal legal label.

Privacy requests and complaints may be sent to ironclad.tournaments@gmail.com.

2. Scope

This Policy applies to the IronClad website, Accounts, profiles, Steam linking, Relic verification, Tournament registration and administration, brackets, Matches, private Match Room communication, rankings, Polls, in-app notifications, deliberately enabled Web Push, installed-app notification badges, support, account closure, optional analytics preference, optional consent-gated public-site analytics and prize administration where applicable.

External providers and sites apply their own privacy notices to processing they perform independently.

This Policy explains IronClad's practices without asserting that every privacy statute applies in every situation. Rights and obligations depend on the applicable law.

3. Information we process

Depending on how a person uses IronClad, we may process:

Account and authentication information:

- Clerk user ID;
- verified email held by Clerk;
- authentication and session state;
- role metadata;
- security and login events; and
- necessary authentication cookies and request metadata.

Profile and contact information:

- display name and in-game name;
- country, region and timezone;

- biography;
- profile visibility settings;
- private avatar object path and mediated public-avatar availability;
- optional Discord username; and
- separate Discord-publication preference.

Steam and Relic information:

- SteamID64;
- Steam persona name;
- Steam-link state and timestamps;
- Relic 1v1 ELO;
- faction;
- Division;
- calculation version; and
- verification timestamps.

Registration and acceptance information:

- registration and Tournament identifiers;
- bracket and Division;
- registration, review and waitlist status;
- immutable registration-time ELO, faction and Division snapshot;
- exact Rulebook, Player Participation Agreement, Terms and Privacy document identifiers, versions, URLs and SHA-256 hashes;
- database-owned acceptance time;
- Rulebook, PPA and Terms acceptance;
- Privacy Policy acknowledgement;
- 18+ declaration; and
- own-IronClad-account and linked-Steam-account declarations.

The acceptance record is private, identity-linked and immutable. It is created atomically with a successful registration. A preliminary waitlist acknowledgement creates neither registration nor acceptance.

Privacy acknowledgement records that the Policy was presented. It is not blanket consent.

Account-wide successor acceptance information:

- authenticated Clerk user ID;
- database-owned acceptance time;
- exact Terms and Privacy document identifiers, versions, stable URLs and SHA-256 hashes;
- Terms acceptance; and
- Privacy Policy acknowledgement.

The account-wide successor acceptance record is private, identity-linked and immutable. It is separate from Tournament registration acceptance and does not record analytics consent.

Tournament and Competition History:

- registrations;

- waitlist and vacancy-offer state;
- brackets and schedules;
- Match participants;
- scores and official results;
- standings and champion records;
- published statistics; and
- related integrity and audit records.

Match, replay and evidence information:

- .rec replay files;
- replay filename, size, path, uniqueness and SHA-256 information;
- upload-attempt and cleanup metadata;
- result submissions;
- confirmation and dispute state;
- no-show reports;
- review notes; and
- proportionate supplemental evidence requested for a genuine dispute or integrity investigation.

Screenshots are not accepted as a substitute for required replay proof.

Dice and Poll information:

- Dice values, Game and tie-round information, participants and timestamps;
- Poll eligibility;
- ballot choices and revisions;
- aggregate totals; and
- final Published Decisions.

Notifications and correspondence:

Match Room information includes message content, sender and room-participant provenance, message order and timestamps, private read positions, unread-notification episodes, Admin Assistance case state, and the minimum audit and retention-control metadata needed to operate and secure that communication.

- in-app notification content and related Event or Match identifiers;
- read, hidden and action state;
- email-delivery status and provider message identifier;
- Web Push subscription endpoint associated with the authenticated Account;
- p256dh and auth cryptographic subscription key material;
- browser notification permission and subscription creation, update, revocation and delivery-failure state where needed;
- the authoritative unread in-app notification count used to reconcile an installed-app badge;
- Admin Assistance requests;
- support and complaint correspondence; and
- privacy, legal and security requests.

Prize information for a prize-bearing Event only:

- prize amount and eligibility;
- supported payout method;
- payout status;
- necessary identity or account-match information;
- transfer and fee information; and
- strictly necessary tax, sanctions or provider-verification information.

IronClad does not currently operate a general payout integration or KYC repository.

A Web Push endpoint and its p256dh and auth key material are linked to an Account and are treated as potentially personal information. IronClad does not collect a device fingerprint, IP address, arbitrary user-agent string, browser history or device name merely to operate Push.

Technical and security information:

Necessary hosting, security and provider logs may contain IP address, device and browser information, timestamps, requested route, response or error metadata, authentication events and security diagnostics.

Analytics preference and optional public-site analytics:

- the first-party browser preference `ironclad_analytics_consent`, containing only granted or declined; and
- when Vercel Web Analytics is enabled and the visitor has selected Allow analytics: a sanitized and normalized approved public route, request timestamp, referrer information limited by IronClad's referrer policy and route redaction, coarse geography, device type, browser, operating system and Vercel's request-derived anonymous daily visitor measure.

Before an analytics pageview may be sent, IronClad removes query strings and URL fragments, normalizes an approved public player-profile route to `/players/[playerId]`, and excludes private, authenticated, operational and unknown routes.

IronClad does not send an IronClad user ID, Clerk ID, SteamID64, email address, Discord username, Match ID, replay or evidence path, custom user property or custom behavioral event to Vercel Web Analytics in this implementation.

Vercel's anonymous visitor mechanism is request-derived and resets daily. It does not identify a globally unique person across days, devices or sites, and IronClad does not describe it that way.

IronClad does not ask for a Clerk, Steam, email or payment password.

4. Sources

Information may come directly from the user, including through a deliberate Enable notifications action; from a delegated Admin acting within authority; from Clerk; from Steam OpenID and Valve's supported public profile service; from Relic's Company of Heroes 3 personal-stat service; from another Player involved in the same Match; from hosting, database, Storage, security and email providers; from the user's browser, operating system and browser-selected Push Service when Web Push is enabled; from a consenting visitor's browser and Vercel for optional public-site analytics when enabled; from support or privacy correspondence; and from a payout provider for a specifically approved prize-bearing Event.

Current profile and registration verification does not send data to COH3Stats. Historical database records may retain a legacy source label.

5. Why we process information

We process information to authenticate users and secure Accounts; create and maintain profiles; verify control of a Steam identity; obtain supported Relic 1v1 information; determine Division eligibility; register and waitlist Players; preserve exact versioned acceptance evidence; operate brackets and Matches; process Dice and Polls; receive and confirm results; investigate disputes, no-shows, cheating and security incidents; calculate rankings and standings; publish factual Competition History; deliver in-app notifications, deliberately enabled Web Push and transactional email; reconcile an installed-app badge with authoritative unread notification state; provide support and Admin Assistance; administer a lawful prize where applicable; prevent fraud and platform abuse; enforce the Governing Documents; maintain required audit and legal evidence; handle account closure and privacy requests; and comply with applicable law.

IronClad preserves private account-wide evidence that an authenticated user accepted the current Terms and acknowledged the current Privacy Policy so it can enforce the required legal-update gate and demonstrate the exact documents presented.

If a visitor opts in and optional analytics has been enabled, IronClad uses the limited analytics information only to measure aggregate public-site traffic, understand which approved public pages are used, and improve the operation and presentation of the website. It is not used for advertising, behavioral profiling, individual eligibility, rankings, Tournament decisions or surveillance.

We do not sell personal information or use private replay evidence for unrelated advertising.

6. Legal grounds where applicable

Where a law such as the GDPR requires a legal basis, the proposed bases are:

- contract and pre-contract steps for Accounts, registration, Event participation, document acceptance and support requested by a user;
- legitimate interests in operating a fair, secure and reliable Tournament platform, preventing fraud, resolving disputes, maintaining proportionate Competition History and protecting legal claims;
- legal obligations where applicable;
- establishment, exercise or defence of legal claims where necessary;
- vital interests only in an exceptional safety situation; and
- consent only where a genuinely optional activity requires it.

Public-profile visibility, public Discord and promotional media are separate choices. Withdrawing an optional choice does not invalidate processing that was already lawful and does not automatically erase factual Competition History.

Privacy acknowledgement is not relied upon as blanket consent.

Where legitimate interests are used, IronClad must consider necessity, proportionality, reasonable expectations and the user's rights.

Optional Vercel Web Analytics relies on the visitor's explicit consent. Analytics is off by default. Declining or withdrawing consent does not block public browsing, Account creation, Tournament registration or participation, or normal IronClad functionality. Withdrawal does not invalidate processing already completed while consent was valid.

7. Authentication

Clerk provides identity, verified email, session, authentication-cookie and role services.

IronClad stores the Clerk user ID where necessary to connect application records. The authenticated identity is derived from the session and is not accepted from an untrusted user-supplied identifier for a privileged operation.

When transactional email is enabled, the verified primary email may be obtained from Clerk at sending time rather than duplicated in the notification table.

8. Profiles, avatars and optional Discord

Profile data supports eligibility, identification, communication and optional public presentation.

Avatar objects are private. The underlying path contains a Clerk user ID, so public delivery is mediated through a player-ID route rather than exposing the private object path.

Discord is optional. A blank value is stored as absent and does not prevent profile completion or registration. Public profile and public Discord are separate opt-ins. Clearing Discord disables public Discord visibility.

A public-profile opt-out does not make official participation anonymous.

9. Steam and Relic verification

Steam linking uses Steam OpenID to establish control of a Steam identity.

IronClad sends the verified SteamID64 to Valve's supported public persona lookup and to Relic's personal-stat endpoint in the form required for the current Company of Heroes 3 lookup.

IronClad stores current verification information on the profile and an immutable ELO, faction, Division, calculation-version and verification-time snapshot when registration succeeds.

SteamID64 is not intended for public-profile display.

Active verification does not use COH3Stats.

10. Registration and durable acceptance

A successful registration is created only after authentication, profile and Steam checks, fresh Relic verification, Division and capacity checks, and the required controls.

The registration and acceptance record commit or fail together.

The acceptance record preserves registration and Tournament identifiers; authenticated Clerk user ID; database-owned timestamp; exact Rulebook, PPA, Terms and Privacy identifiers, versions, stable URLs and SHA-256 hashes; Rulebook, PPA and Terms acceptance; Privacy acknowledgement; 18+ declaration; and own-Account and linked-Steam ownership declarations.

Document identifiers supplied by the browser are treated only as selectors. The trusted server and database load and verify the authoritative document status, version, URL and hash.

Acceptance evidence is private and is not a public profile or Competition History field.

A separate account-wide successor acceptance record may be required when Effective Terms or Privacy versions change materially. It records the authenticated Clerk identity, database-owned time, exact Terms and Privacy document identifiers, versions, stable URLs and SHA-256 hashes, Terms acceptance and Privacy acknowledgement. It is private and immutable, does not create or amend a Tournament registration, and does not record optional analytics consent.

11. Match results and private evidence

One unique .rec file for each Game actually played is the required Match-result proof.

Replay uploads use private Storage, signed upload authorization, size and filename controls, uniqueness checks and server-side metadata validation.

Replay objects, raw paths, hashes, disputes, no-show material, private notes and supplemental evidence are limited to involved Match participants where necessary for the result and dispute process; delegated Admins acting within authority; necessary service providers; and persons legally entitled to receive them.

Scores and official results may become public. Private evidence does not become promotional content.

Match Room messages are private communication between the two authorized room participants. Authorized IronClad tournament administrators may access retained messages for tournament operations, Admin Assistance, disputes, moderation, competition integrity and safety. Public visitors and unrelated players cannot access the private transcript or another participant's read state.

Access follows the current authoritative Match, room membership, Account and administrator permissions. A reset, reassignment, completed Match, closed Account or disabled communication feature may restrict access or make a room read-only; these changes do not turn the transcript into public content.

Users may place personal information in free text. Removing or pseudonymising an Account identifier does not automatically anonymise message bodies. Users should avoid unnecessary personal information about themselves or others.

Screenshots are not accepted as a substitute for required replay proof. They may be considered only as proportionate supplemental material for a genuine dispute or integrity investigation.

12. Dice and Polls

Dice history is available to the relevant Match participants and read-only Admin contexts.

Poll eligibility is frozen when a Poll is published. An eligible Player may see their own choices and aggregate totals only according to the Poll's live or after-close setting.

Individual ballot attribution is private. Anonymous public totals exist only when explicitly enabled. Final Published Decisions may be public.

Poll finalization does not automatically mutate another subsystem.

13. Notifications, email and Admin Assistance

IronClad stores in-app notification content, related identifiers, read or hidden state and action state.

Web Push is optional and may be enabled only through a deliberate signed-in user action followed by the browser's notification-permission process. IronClad does not request notification permission automatically when a page loads. Browser notification permission is a technical permission and is not blanket consent to unrelated processing.

Each subscribed browser or installed web application has its own standards-based PushSubscription. One Account may have multiple subscriptions. IronClad stores the minimum endpoint, p256dh and auth values needed for encrypted delivery and does not use Firebase or a paid Push provider for this feature.

Web Push is a best-effort delivery channel for selected meaningful notification events. The in-app notification record remains authoritative. The installed-app badge is reconciled from the Account's authoritative unread in-app notification count, even where an unread notification was not Push-important. Platform support may present an exact number, a dot or no badge.

Push content may be visible on a lock screen. IronClad therefore limits payloads to a conservative title, concise event summary, notification identifier, approved same-origin destination and an unread-count snapshot. It does not include replay or private Storage URLs, private evidence, email addresses, raw identity data, sensitive Admin notes or full dispute contents.

When transactional email is enabled, Resend receives the verified recipient email, subject, HTML or text content, sender and reply-to information, and delivery/idempotency metadata necessary to send and audit the message.

The Gmail mailbox receives messages sent to the published support, privacy and legal address.

A participant-scoped Admin Assistance request stores the requesting identity, relevant Match and notification state needed to prevent duplicate open requests and allow delegated Admin follow-up.

14. Public information and Competition History

Depending on Event and visibility settings, public information may include opted-in profile fields, public avatar presentation, optional public Discord, approved or bracketed competition name, registration and bracket facts, scores and official results, standings and champion records, final Published Decisions, and explicitly enabled anonymous Poll totals.

Turning off a public profile or closing an Account does not automatically remove factual Competition History.

After closure, retained history may use "Former Competitor" and suppress the closed player's profile identifier, location, live ELO, avatar and optional contact fields.

Public information is accessible internationally and may be copied or indexed by others outside IronClad's control.

15. Providers and recipients

Current and conditional providers and recipients are:

- Marco Stucchi and Simone Vitiello: the two responsible natural-person operators, with access from New South Wales and Italy as required to operate the Service.
- Delegated Admins: operational personnel, not included in IronClad/we/us/our and not responsible operators merely because of their role; access is limited to authorized support, Event and integrity functions.
- Clerk: current authentication, identity, verified email, sessions, role metadata and necessary authentication cookies.
- Supabase PostgreSQL and Storage: current profiles, registrations, acceptances, Matches, Polls, rankings, notifications, avatars, replay evidence and audit state.
- Vercel: current hosting, application delivery and request processing and, only when enabled after the visitor's separate opt-in, optional public-site Web Analytics.
- Browser and operating-system Push Services: conditional, only after deliberate account-level enablement, to route encrypted standards-based Web Push to each subscribed browser or installed web application. The browser or operating system selects that service and its infrastructure or subprocessors.
- Valve/Steam: current Steam OpenID and supported public persona lookup.
- Relic: current Company of Heroes 3 competitive lookup.
- Resend: transactional email when enabled for a message.
- Google/Gmail: the published support, privacy and legal mailbox.
- Discord: optional external communication only; no current IronClad API or bot integration.
- Wise, PayPal or another published provider: conditional, only for an approved prize-bearing Event.

COH3Stats is not a current provider for active verification.

Battlefy is not a current registration or result authority. A clearly historical outbound link, if displayed, is an external link rather than a transfer used to administer the current Event.

16. International processing

IronClad does not promise that personal information is stored only in Australia or only in the European Economic Area.

The responsible operators may access Service data from New South Wales and Italy. Current providers and their subprocessors may process information in other countries according to their infrastructure, account configuration and contractual arrangements.

When Web Push is deliberately enabled, the browser-selected Push Service and its relevant infrastructure or subprocessors may process the subscription endpoint, encrypted delivery data and routing metadata in countries outside the user's country. IronClad must review applicable provider terms and transfer safeguards before activation.

Public Competition History is accessible globally.

Where applicable law requires a transfer safeguard, IronClad must use an appropriate legal or contractual mechanism before relying on that transfer or must stop the affected processing. Disclosure in this Policy is not itself a transfer mechanism.

Provider regions, subprocessors, data-processing terms and transfer mechanisms must be reviewed periodically and when a provider changes.

When optional Web Analytics is enabled after consent, Vercel and its relevant infrastructure or subprocessors may process the limited analytics information in countries outside the visitor's country. This disclosure does not claim a legal certification or by itself establish a transfer mechanism.

17. Cookies, session storage and tracking

IronClad currently uses:

- Clerk authentication and session cookies for sign-in, session continuity, security and authorization. Duration is provider-managed under the configured Clerk session and cookie settings.
- `__Host-ironclad-steam-link`, a necessary first-party cookie that binds a Steam OpenID callback to the authenticated session and linking intent. It lasts up to 10 minutes, contains random flow state, intent, session hash and expiry, is `HttpOnly`, `Secure`, `SameSite=Lax` and `Path=/`, and is cleared by the callback.
- `ironclad_locale`, a first-party functionality-preference cookie that remembers only the selected interface locale. It lasts up to one year, is `HttpOnly`, `SameSite=Lax` and `Path=/`, and is `Secure` in Production. For a signed-in user, the selected transactional-language preference may also be mirrored in Clerk private metadata. This preference is separate from analytics consent and is not used to measure behavior.
- `ironclad:new-tournament-draft` in browser `sessionStorage` to recover non-file fields in the delegated Admin create-Tournament form. It is scoped to the browser tab/session and excludes the file input and stored banner image URL.
- `ironclad_analytics_consent` in browser `localStorage`, containing only granted or declined, solely to remember the visitor's optional analytics preference. It contains no user ID, account ID, email, Steam identity, IP address, fingerprint or preference-history timestamp.
- a standards-based browser `PushSubscription`, created only after a deliberate enable action and browser permission, containing an endpoint and `p256dh` and auth key material. IronClad stores the subscription against the authenticated Account; the browser or operating system controls its own permission and local service-worker state.

Apart from the analytics preference described above, IronClad does not use application `localStorage` for analytics, a marketing cookie, an advertising pixel or a general consent-management platform. The preference remembers the visitor's choice and is not itself used to measure behavior.

Web Push permission and subscription state are used only to deliver opted-in notifications and reconcile the installed-app badge. They are not used for advertising, cross-site tracking or device fingerprinting. Browser notification permission is a technical permission and is not blanket consent to unrelated processing.

Clerk, Vercel and other providers may create necessary security, request and diagnostic logs. Those logs are not described as advertising tracking.

Optional analytics is off by default. The focused analytics choice presents Allow analytics and Decline without a preselected choice. Declining does not reduce normal IronClad functionality. A visitor may later change or withdraw the preference through the Analytics choices control.

When Vercel Web Analytics is enabled in a later controlled release, it may load only after the stored preference is granted. Vercel Web Analytics does not set an analytics cookie. IronClad limits collection to an explicit public-route allowlist, removes query strings and URL fragments, normalizes approved public player-profile routes, applies a

protective referrer policy, and fails closed for private, authenticated, operational and unknown routes. No custom analytics user properties or custom behavioral events are used in V1.

Any later analytics expansion, advertising, cross-site measurement or embedded tracking requires a fresh data-minimisation and Policy review and any legally required choice before it loads. Reject and withdrawal controls must remain as accessible as acceptance where consent is required.

Traffic reports may undercount because visitors can decline or withdraw analytics and because JavaScript blocking or ad blockers may prevent collection.

18. Retention

IronClad retains information only for the operational, integrity, contractual, security, legal and historical purposes described below.

Information	Retention and disposition
Active profile, avatar, current Steam/Relic state and optional Discord	For the life of the Account. On completed closure, delete or clear from live profile systems except the minimal pseudonymised historical shell.
Rejected, withdrawn, expired-waitlist, abandoned or non-launched registration	12 months from final status, then delete or deidentify unless an active complaint, fraud investigation or legal hold applies.
Approved registration snapshot and factual Competition History	Indefinite factual archive, retaining the minimum factual record and pseudonymising on closure where direct identity is no longer necessary.
Immutable registration acceptance	7 years from the database acceptance timestamp. Account closure does not shorten this period. Delete through controlled legal-evidence maintenance unless an active claim or legal hold requires longer retention.
Immutable account-wide successor acceptance	7 years from the database acceptance timestamp. Account closure does not shorten this period. Delete through controlled legal-evidence maintenance unless an active claim or legal hold requires longer retention.
Raw .rec replay, dispute, no-show and supplemental integrity material	24 months after the result becomes final, then delete the object and unnecessary linked metadata unless an active integrity or legal hold applies.
Replay hash after raw-file deletion	Delete with the replay by default; retain up to 7 years only where a documented integrity or legal-evidence purpose remains, then delete when that purpose ends.
Upload-attempt and abandoned-object metadata	90 days after completion, failure or cleanup, then delete.
Dice history	24 months after Match finalization, then delete or deidentify unless an active integrity hold applies.
Poll voter attribution and individual choices	12 months after the final decision, then delete or deidentify individual attribution and choices where practicable.
Final anonymous Poll aggregates and Published Decisions	Indefinite factual archive without individual ballot attribution.
In-app notifications	12 months after becoming non-actionable, then delete or deidentify unless part of another retained case record.
Routine private Match Room communication	Retain message content for 40 days after the Tournament officially closes, using its authoritative current completed, cancelled or voided state and trustworthy closure time. This period does not start when an individual Match ends. Expired routine content and unnecessary communication-only attribution are removed through bounded, documented maintenance; a minimal non-content room identity and necessary competitive provenance may remain.
Match Room material linked to a formal case or investigation	Apply the existing relevant longer period: 24 months after support, complaint, privacy or Admin Assistance case closure; or 24 months after the result becomes final for dispute, no-show or supplemental competition-integrity material. An active case or applicable narrow hold prevents deletion of affected material. Association is determined by authoritative case or system records, never by classifying message text.

Information	Retention and disposition
Web Push subscriptions	For the life of the deliberate Push opt-in. Delete when the user disables Push in IronClad, on completed Account closure, or when a Push Service reports an expired or invalid endpoint, including HTTP 404 or 410. If permission is revoked only in the browser or operating system, delete when IronClad next detects the revocation or delivery failure. Provider copies follow the provider's lawful schedule.
Transactional-email delivery audit	12 months after the final delivery attempt, then delete IronClad's audit copy subject to the provider's independent retention.
Support, complaint and privacy-request cases	24 months after case closure, then delete unless an active legal, regulatory or security hold applies.
Security and runtime logs under IronClad control	No more than 90 days where configurable, unless needed for an active incident.
Optional analytics preference and Vercel Web Analytics	The granted or declined preference remains in that browser until the visitor changes it or clears browser storage. When analytics is enabled after consent, Vercel Hobby reporting available to IronClad covers a rolling one-month window. Vercel may retain provider copies under its own lawful schedules, so IronClad does not promise automatic deletion at exactly 30 days.
Backup and point-in-time-recovery copies under IronClad control	A maximum rolling window of 90 days. Allow copies to age out, do not use expired copies for ordinary access, and reapply completed deletion and pseudonymisation after restoration.
Prize, payment and accounting records	7 years after payment or final resolution, or longer where law requires, then delete or deidentify non-required material.
Identity documents collected for a necessary check	Do not routinely collect; if temporarily received, delete within 30 days after the check finishes unless a specific law, provider requirement, dispute or legal hold requires longer retention.

A legal, security or integrity hold suspends deletion only for affected information and only for as long as reasonably necessary. After a hold ends, overdue deletion should occur within 30 days.

A Match Room hold must identify affected material and a documented legal obligation, security, abuse/safety or competition-integrity purpose. Holds are reviewed and released when the purpose ends. Routine conversation is not retained indefinitely by default; after release, normal purge eligibility resumes.

Retention is evaluated against current authoritative state. If a Tournament legitimately reopens, a stale closure date is not used for deletion. If no trustworthy closure timestamp exists, maintenance stops for that material and requires an authority review rather than inventing a date or treating unrelated timestamps as closure.

Communication cleanup does not delete Tournament results, brackets, registrations, standings or required immutable competitive history. Minimal non-content tombstones and audit counts support safe retries, prevent transcript recreation and record the class of data removed without logging message bodies.

Time-based cleanup may be performed through documented operational review rather than an automated scheduler. The absence of automation does not lengthen the stated period.

Providers may retain independent copies under their own lawful schedules. IronClad must send a deletion request where appropriate but cannot promise immediate deletion from every provider or backup.

Deidentified information that can no longer reasonably identify a person may be retained for statistics, integrity analysis and historical reporting.

19. Account closure and deletion

A user may request closure through the profile process or contact email.

The current sequence is:

1. remove the private avatar;
2. invoke the database closure process; and

3. request Clerk account deletion.

The systems do not form one transaction. One step may succeed while another fails. IronClad must record and reconcile a known partial failure.

On completed Account closure, IronClad deletes active Web Push subscription rows associated with that Account. Browser or operating-system permission and provider-side routing state may not disappear immediately; detected expired or invalid endpoints are removed under the retention schedule.

Where no protected Competition History exists, the player record may be deleted. Where history exists, direct profile identifiers and optional contact fields are removed or neutralized; current Steam and Relic state is cleared; live ELO, biography, avatar and visibility preferences are removed; historical actor identifiers are pseudonymised where supported; and factual history may remain as "Former Competitor".

Immutable acceptance remains identity-linked for its seven-year period.

Private replay, integrity, Dice, Poll and correspondence material follows the retention schedule.

Completed Account closure immediately revokes future Match Room access and messaging through the existing closure authority, removes private read state and clears direct Account-linked communication and notification attribution as supported by that architecture. Retained free-text messages are not represented as anonymised.

Routine retained messages remain subject to 40 days after Tournament closure. Account closure does not automatically override a valid temporary formal-case, integrity, security or legal retention requirement; affected material follows the applicable longer schedule and hold review.

Free-text or replay content may contain information not automatically discoverable by structured closure. IronClad will review specifically identified material where a substantiated request or legal obligation requires it.

External providers, mailboxes, logs and backups may not disappear immediately. Completed deletion obligations must be reapplied if an older backup is restored.

20. Privacy choices and rights

Depending on applicable law, a person may request access, correction, deletion, restriction, portability, objection, withdrawal of a genuinely optional consent, Account closure, changes to public-profile or public-Discord settings, and information about applicable disclosures or transfers.

A request may be sent to ironclad.tournaments@gmail.com.

IronClad may verify identity proportionately. It will not request a password or authentication code. Additional evidence should be requested only where reasonably necessary.

For a substantiated Match Room access, export or erasure request, an authorized operator can locate retained records using verified Account or historical player provenance. Any export is limited to the requester's own rooms and reviewed for another person's rights before secure delivery. Authorized targeted deletion or redaction is assessed against active cases, lawful holds and the retention schedule; it does not erase unrelated rooms or competitive history.

A retained export is handled as private case material. Live-system deletion does not instantly erase older backup copies: the existing maximum rolling 90-day backup window applies, expired copies are excluded from ordinary access, and completed deletion or pseudonymisation obligations must be reapplied after restoration.

A right may be limited by another person's rights, a legal obligation, security, fraud prevention, an active claim, or a justified competition-integrity or factual-history need. IronClad should explain a refusal or partial response and identify an available complaint route.

Withdrawing public-profile, Discord or media permission does not automatically erase lawful historic publication or affect processing already completed on another valid basis.

A visitor may change or withdraw the optional analytics preference through the Analytics choices control. Declining or withdrawing analytics does not affect normal access to IronClad. Clearing browser storage may remove the saved choice, in which case analytics remains off until another deliberate choice is made.

A signed-in user may choose whether to enable Web Push, may disable it in IronClad, and may revoke notification permission in the browser or operating system. Refusing or disabling Push does not remove ordinary in-app notifications or affect Tournament eligibility. Badge appearance and exact numeric presentation depend on platform support.

21. Rules-based processing and human review

IronClad uses deterministic rules for ELO-based Division, registration capacity and FIFO waitlist order, replay-count and upload checks, confirmation deadlines, result auto-confirmation, ranking calculations and Poll finalization.

These rules use published criteria and platform state. Relevant errors, disputes and sanctions have a delegated Admin review route.

IronClad does not use AI to make autonomous competitive, payout, sanction or moderation decisions.

Where applicable law treats a rule as a solely automated decision with legal or similarly significant effect, IronClad will provide the notice and human-review rights that law requires.

22. Security and incidents

Safeguards include Clerk authentication, server-side authorization, role controls, PostgreSQL row-level security, private Storage, signed uploads, mediated replay and avatar delivery, service-role isolation, SHA-256 integrity checks, restricted database grants, trusted server timestamps and server-side validation.

Acceptance records and the legal-document register are private. Public, anonymous and ordinary authenticated database roles cannot directly mutate them.

No system is perfectly secure. IronClad does not promise that a breach or failure can never occur.

IronClad must maintain a proportionate incident process covering triage, containment, provider coordination, evidence preservation, risk assessment, recovery and legally required notifications.

A suspected security incident may be reported to ironclad.tournaments@gmail.com without including passwords or authentication codes.

23. Age

Tournament registration is restricted to persons aged at least 18.

Registration records the Player's 18+ declaration. IronClad does not routinely collect identity documents merely to register.

Any additional age verification must be necessary, proportionate and privately handled under the retention schedule.

24. External links and services

Discord, Steam and clearly historical Battlefy links lead to external services. A prize provider also applies its own terms and privacy notice.

IronClad is not responsible for unrelated processing a person initiates directly with an external service, but it remains responsible for accurately describing information IronClad itself sends to that service.

25. Changes and versions

Every Effective Privacy Policy has a version, publication date, effective date and stable version-specific URL.

A material change must not overwrite the existing version. IronClad must provide appropriate notice and obtain renewed acknowledgement or consent where applicable.

A material change includes a significant new purpose, recipient, public disclosure, retention period, tracking technology, transfer arrangement or reduction in rights.

Privacy acknowledgement records delivery of the notice. It is not blanket consent.

26. Contact and complaints

Privacy enquiries, requests and complaints may be sent to ironclad.tournaments@gmail.com.

A request should describe the relevant Account or activity and the requested outcome. It must not include passwords, authentication codes or unnecessary identity documents.

IronClad should acknowledge and respond within the period required by applicable law.

A person may complain to a competent privacy or consumer authority where applicable, including an authority connected with the person's location or the relevant responsible operator. Use of that route does not depend on first accepting IronClad's preferred outcome.

English is the controlling language of this version. A translation is informational unless separately identified as legally authoritative. Mandatory local-language rights remain unaffected.

END OF PRIVACY POLICY v1.3