
Terms of Service

Effective August 3, 2026 · Defy Technologies Pte Limited · Downloaded September 10, 2026 at 11:02 PM Fiji Standard Time

1. Definitions

In these Terms of Service ("Terms"), the following words have the meanings below:

- **"Defy", "we", "us", "our"** — Defy Technologies Pte Limited, a company operating from 58 Link Road, Lautoka, Fiji (P.O. Box 2521, Lautoka).
- **"Customer", "you", "your"** — the person or organization that holds a Defy account or is party to a service agreement with Defy.
- **"Services"** — collectively, Managed Services, Cyber Security, IT Consulting & Advisory, Web and Mobile Development, and the Defy Cloud Platform (domains and DNS, hosting and compute, email hosting, SSL certificates, networking, and software licensing).
- **"Cloud Platform"** — the subscription infrastructure services accessed through Defy Console, Defy Billing, and Defy Accounts, as distinct from project-based or managed engagements governed by a separate service agreement.
- **"Managed Environment"** — infrastructure, hardware, or software that Defy has agreed in a Service Agreement to actively monitor, maintain, or administer on your behalf, as distinct from infrastructure you operate yourself.
- **"Customer Data"** — any data, content, or material you or your Authorised Users submit to, or generate through, the Services.
- **"Authorised User"** — an individual you permit to access the Services under your account.
- **"Service Agreement"** — a signed statement of work, order form, or managed services agreement between you and Defy.
- **"Force Majeure Event"** — an event outside a party's reasonable control, as described in Section 23.
- **"Business Day"** — a day other than a Saturday, Sunday, or public holiday observed in Fiji.

2. Acceptance of Terms

By creating a Defy account, signing a Service Agreement, or otherwise using the Services, you enter into a binding agreement with Defy on these Terms. You must be at least 18 years old and have the legal capacity to enter into this agreement. If you are agreeing on behalf of a business or other organization, you confirm you have the authority to bind that organization, and "you" refers to that organization.

Where a signed Service Agreement conflicts with these Terms, the Service Agreement governs for the matters it specifically addresses; these Terms continue to apply to everything else.

We may amend these Terms from time to time. Material changes take effect no sooner than 30 days after we give you written notice (by email or through the Services), except where a change is required to comply with law or to address an active security risk, in which case it may take effect immediately with notice given as soon as reasonably practicable. Continued use of the Services after a change takes effect constitutes acceptance.

3. Licence Grant & Restrictions

Subject to these Terms and payment of applicable fees, Defy grants you a limited, non-exclusive, non-transferable, non-sublicensable, revocable licence to access and use the Services for your internal business purposes.

You must not, and must not permit any Authorised User or third party to:

- Reverse engineer, decompile, or attempt to derive the source code of any Defy platform software;
- Sublicense, resell, or provide the Services to a third party as a standalone offering, except where you are an agency or reseller under a separate written agreement with Defy;
- Circumvent or attempt to circumvent any authentication, rate-limiting, or security control on the Services; or
- Use the Services to build a directly competing product.

4. Onboarding

Where you engage Defy for Managed Services, or move existing infrastructure into a Managed Environment, onboarding generally follows these steps:

- **Discovery & documentation** — we inventory the hardware, software, credentials, and network topology relevant to the engagement.
- **Baseline review** — a lightweight check of patch status, exposed services, and existing backup coverage, performed before Defy assumes ongoing management responsibility, so both parties have a documented starting state.
- **Access provisioning** — administrative access is requested and granted on the least-privilege basis described in Section 6; any temporary elevated access used specifically for migration is revoked once onboarding is confirmed complete.
- **Monitoring & tooling deployment** — monitoring agents and management tooling are installed and validated as working before being relied on.
- **Handover confirmation** — written confirmation of exactly what is now inside the Managed Environment, and what, if anything, remains your responsibility.

Onboarding timelines depend on the size and condition of the environment being brought under management and are agreed as part of the Service Agreement, not fixed by these Terms.

5. User Responsibilities & Data Accuracy

You are responsible for the accuracy of information you submit to the Services, including domain registrant details, billing details, and any configuration data you enter into Console. Where the Services generate reports, invoices, or other outputs derived from data you or your integrations provide (for example, usage or billing summaries), those outputs are only as accurate and complete as the underlying data — Defy is not responsible for decisions made on the basis of incomplete or inaccurate Customer Data.

You are responsible for the conduct of your Authorised Users and for ensuring they comply with these Terms, including the Acceptable Use Policy in Section 17.

6. Access Control & Password Policy

Defy Accounts supports multi-factor authentication via authenticator app or passkey, and mandatory enrollment is enforced platform-wide. You are responsible for keeping your login credentials and registered MFA method confidential, and for all activity under your account. Where you or your Authorised Users manage systems we don't administer ourselves, we strongly recommend the same standard: MFA wherever it's supported, and unique credentials per person rather than shared logins.

For any Managed Environment, Defy applies the following internally:

- **Least privilege** — staff and automated tooling are granted only the access needed to perform a given task, not standing access to everything by default.

- **No shared credentials** — Defy does not use generic or shared administrative accounts across customers; access is attributable to an individual or a specific automated process.
- **Periodic review** — standing administrative access to a Managed Environment is reviewed on a reasonable schedule, and revoked promptly when no longer needed — including immediately upon a change in which staff member holds it.
- **One-off task credentials aren't retained** — where you provide a credential for a single task (for example, a manual deployment), it is encrypted while the task runs and is not kept afterward.

Defy staff will never ask you for your account password, MFA codes, or a domain registry auth code over phone, email, or chat. Report suspected unauthorized access or a compromised credential immediately to support@defy.com.fj.

7. Service Levels, Support Tiers & Availability

Support response targets depend on the tier included in your Service Agreement and the severity of the issue. These are targets for initial response and engagement, not guarantees of a fixed resolution time — resolution depends on the nature of the underlying problem, including factors outside Defy's control such as a third-party vendor's own response time.

Severity	Standard tier	Priority tier
1 — Critical (complete outage, active security incident)	4 business hours, 24/7 phone escalation available	1 hour, 24/7
2 — High (major degradation, workaround exists)	1 Business Day	4 business hours
3 — Normal (limited impact)	2 Business Days	1 Business Day
4 — Low (general request, minor/cosmetic)	3 Business Days	3 Business Days

"Standard tier" reflects business-hours coverage (Monday-Friday, 8am-5pm Fiji Standard Time). "Priority tier" is an upgraded Managed Services plan with extended coverage; exact hours and whether Priority applies to your account are set out in your Service Agreement.

For Cloud Platform infrastructure (hosting and compute services), Defy separately targets 99.9% monthly uptime, measured at the platform level — approximately 43.8 minutes of permissible unplanned downtime per month. This target excludes scheduled maintenance (see Section 18), emergency maintenance to address an active security risk, Force Majeure Events, and outages originating solely from a third-party infrastructure provider's own network or hardware outside Defy's control. This is a service target, not a guaranteed credit-backed SLA, unless a specific service level agreement with defined remedies is set out in your Service Agreement.

8. Change Management Policy

For any infrastructure inside a Managed Environment:

- **Routine changes** — low-risk work such as patching within an agreed maintenance window, or minor configuration adjustments, may be carried out without a separate approval step each time, consistent with the maintenance schedule disclosed under Section 18.
- **Major changes** — anything with a realistic risk of service disruption, including infrastructure migrations, firewall rule changes, DNS cutovers, or software upgrades with known breaking changes, requires your prior approval (email is sufficient) before being carried out.

- **Emergency exception** — the approval step above may be bypassed where a change is urgently required to contain an active security incident under Section 9 (Incident Response Plan); in that case we notify you as soon as reasonably practicable after the fact, not before.

Where practical, major changes are tested in a non-production environment or scheduled during an agreed maintenance window, with a documented rollback plan.

9. Incident Response Plan

In the event of a suspected security incident, data breach, or significant failure affecting a Managed Environment or Cloud Platform infrastructure:

- **Detection & containment** — on detection (by our monitoring or your report), we take immediate steps to contain the issue and limit further impact.
- **Notification** — we notify you as soon as reasonably practicable, and without undue delay where the incident involves a confirmed compromise of personal data, consistent with the Privacy Policy.
- **Investigation** — a root cause investigation to determine scope and impact.
- **Remediation** — resolving the immediate issue and, where relevant, hardening against recurrence.
- **Post-incident report** — for significant incidents, a written summary of what happened, what was affected, and what's changed as a result, provided on request.

Report a suspected incident immediately to support@defy.com.fj or 999 1688. Severity 1 incidents are escalated 24/7 regardless of your support tier.

10. Data Hosting, Privacy & Security

Cloud Platform infrastructure runs on a global cloud compute network operated by our infrastructure partner. For compute (VPS) services, your server is provisioned in the region you select at checkout; Defy does not relocate your data to a different region without your action. Shared hosting runs on Defy-operated hosting infrastructure.

Data in transit to and from the Services is encrypted using TLS. Sensitive stored data — including identity verification documents — is encrypted at rest using AES-256. Access to administrative and customer-data systems requires multi-factor authentication and is scoped by role, consistent with Section 6.

Further detail on what personal data we collect and how it's used is set out in our [Privacy Policy](#).

11. Data Retention & Backup Policy

We retain Customer Data for as long as your account remains active. If an account is suspended for non-payment or a Terms violation, associated data is retained for 6 months from suspension to allow for reinstatement, after which it may be permanently deleted. Billing and tax records are retained for the period required by applicable law regardless of account status.

Where you add automated backups to a compute plan at checkout, backups run on the schedule and retention our infrastructure partner provides for that service. For customers under a Managed Services engagement that includes backup oversight, we periodically verify that backup jobs are completing successfully and, on a reasonable schedule, that a sample restore is actually achievable — not merely that a job reported success. Backups are a safety measure, not a guarantee: you should maintain your own copies of data where the impact of loss would be severe.

12. Data Export & Exit Rights

You may request an export of your Customer Data at any time while your account is active. For a planned exit from an ongoing Managed Services or Cloud Platform engagement, we ask for 30 days' written notice so the export can be scheduled without disrupting production services; exports are typically ready within 30 days of the scheduled export date, in a standard, documented format appropriate to the service (for example, a database dump for hosted applications, or a zone file for DNS records).

Domain names remain your property and are portable — we will provide the transfer authorization code for any domain registered through us on request, subject to the registry's own transfer rules.

Following termination, data may remain in an inaccessible, non-production state for a further 90 days after your export window closes (to allow recovery from an accidental termination request) before permanent deletion from active systems.

13. Offboarding

When a Managed Services or Cloud Platform engagement ends, in addition to the data rights in Section 12:

- **Access revocation** — all administrative access Defy holds to your systems (VPN, remote management tools, admin accounts) is revoked within 5 Business Days of termination taking effect, unless a transition period is separately agreed.
- **Credential handover** — where you request it, credentials for accounts or systems that need to remain under your control are provided to you, not simply deleted, as part of the transition.
- **Equipment & access tokens** — any Defy-provided hardware, physical access tokens, or similar is returned or deactivated.
- **Final documentation** — a summary of the infrastructure and configuration as it stood at handover, so a new provider or your own team isn't starting blind.

14. Vendor & Third-Party Risk Policy

Defy relies on a limited set of vetted infrastructure and software vendors to deliver the Services — including cloud compute and networking, business email delivery, domain registration, and payment processing (see Section 10 and our [Privacy Policy](#) for how data is shared with them).

Before relying on a new vendor for a function that touches Customer Data or production infrastructure, we consider that vendor's security practices and track record. We monitor our vendors' status pages and security advisories for issues that could affect the Services, and each vendor is only given access to what's necessary for the specific function it performs for us — not broad access to Customer Data generally.

15. Billing, Payments & Subscriptions

Cloud Platform subscription fees are billed in advance through Defy Billing on the cycle disclosed at checkout. Invoices are due within 14 days of issue unless your Service Agreement states otherwise. We will give at least 60 days' advance written notice of a pricing change to an active subscription. Fees exclude VAT unless stated otherwise.

Card and bank payment details are collected and processed directly by our third-party payment gateway — Defy does not store your full card number on its own servers.

An account more than 14 days overdue may be suspended after notice. A domain registration that lapses due to non-payment may become unavailable for renewal once released by the registry, and Defy is not liable for loss of a domain name due to non-renewal.

16. Refund Policy

Setup, migration, and other one-time project fees are non-refundable once work has commenced. Cloud Platform subscription fees are non-refundable except where Defy fails to remedy a material service failure within a reasonable time after you notify us, in which case a pro-rata credit may apply for the affected period. Domain registration and renewal fees are non-refundable once submitted to the registry, consistent with registry policy. Refunds, where applicable, are processed within 14 Business Days of approval.

17. Acceptable Use Policy

You must not use the Services to:

- Host, transmit, or distribute unlawful, infringing, fraudulent, or malicious content, including malware;
- Send unsolicited bulk email ("spam"), or otherwise abuse email or hosting infrastructure in a way that damages Defy's or a third party's network reputation;
- Attempt unauthorized access to any system, scrape or overload a service, or otherwise interfere with the integrity of Defy's or another party's infrastructure;
- Conduct phishing or impersonation using Defy-provided infrastructure; or
- Violate the acceptable use policies of Defy's underlying infrastructure providers, which apply to your use of services built on top of them.

A material breach of this section may result in immediate suspension of the affected service, and, where the conduct is unlawful, referral to the appropriate authorities.

18. Technical Support & Maintenance

Response and resolution targets by tier and severity are set out in Section 7. Phone and chat support are available Monday-Friday, 8am-5pm Fiji Standard Time for Standard tier; extended hours for Priority tier are set out in your Service Agreement.

Routine maintenance affecting Cloud Platform infrastructure or a Managed Environment is scheduled outside Fiji business hours where practicable, with advance notice through the Services or by email, consistent with the Change Management Policy in Section 8.

19. Confidentiality

Each party will use the other's confidential information only to perform its obligations under these Terms or an applicable Service Agreement, and will protect it with at least the same care it uses to protect its own confidential information of similar importance. This obligation survives termination of the relationship for 5 years, except for information that constitutes a trade secret, which remains protected for as long as it retains that status.

This section does not apply to information that is or becomes publicly available through no fault of the receiving party, or that must be disclosed by law, provided the disclosing party gives notice where legally permitted.

20. Representations & Warranties

Defy warrants that the Services will perform materially in accordance with their published documentation. You warrant that you have the authority to enter into these Terms, that your use of the Services will comply with applicable law, and that you

own or have the necessary rights to Customer Data you submit.

Except as expressly stated in this section or a signed Service Agreement, the Services are provided "as is" and "as available", and Defy disclaims all other warranties, including implied warranties of fitness for a particular purpose and uninterrupted or error-free operation, to the maximum extent permitted by law.

21. Limitation of Liability

To the maximum extent permitted by law, neither party is liable to the other for indirect, incidental, consequential, or special damages, including loss of profits, loss of revenue, or loss of business, arising out of or relating to these Terms or the Services.

Defy's total aggregate liability arising out of or relating to the Services will not exceed the total fees you paid to Defy for the specific service giving rise to the claim in the 3 calendar months immediately preceding the event. This limitation does not apply to liability that cannot be excluded by law, including liability for death or personal injury caused by negligence, or for fraud.

22. Term & Termination

Subscription services renew automatically for successive terms matching your billing cycle unless either party gives at least 30 days' notice of non-renewal before the next renewal date. For ongoing Managed Services or Cloud Platform engagements without a fixed term, either party may terminate with 30 days' written notice, or immediately for the other party's uncured material breach following 30 days' written notice of that breach.

Defy may suspend or terminate access immediately, without the cure period above, for non-payment after notice under Section 15, a violation of Section 17 (Acceptable Use), or where continued provision would expose Defy or other customers to legal or security risk. Defy may also terminate on notice if you become insolvent or enter administration or liquidation. Data handling and access revocation following termination are governed by Sections 11-13.

23. Force Majeure

Neither party is liable for a failure or delay in performance caused by events outside its reasonable control, including acts of God, war, civil unrest, pandemic, government action, and cyberattacks of exceptional scale directed at critical infrastructure providers rather than a result of either party's own security failure. If a Force Majeure Event continues for more than 60 consecutive days, either party may terminate the affected Service Agreement without further liability, other than payment for fees already accrued.

24. Dispute Resolution

If a dispute arises out of or relating to these Terms or the Services, the parties will first attempt in good faith to resolve it through direct negotiation between authorized representatives for at least 14 days. If unresolved, the parties will attempt non-binding mediation in Suva, Fiji, with the cost of the mediator shared equally, before either party commences court proceedings.

These Terms are governed by the laws of the Republic of Fiji, and any dispute not resolved under this section is subject to the exclusive jurisdiction of the courts of Fiji.

25. General Provisions

Entire agreement. These Terms, together with any applicable Service Agreement and our [Privacy Policy](#), constitute the entire agreement between you and Defy regarding the Services, superseding any prior discussions or agreements on the same

subject.

Severability. If any provision of these Terms is found unenforceable, the remaining provisions continue in full effect, and the unenforceable provision will be interpreted to best reflect its original intent.

Waiver. A failure to enforce any provision is not a waiver of the right to enforce it later.

Assignment. You may not assign or transfer your rights under these Terms without Defy's prior written consent. Defy may assign these Terms in connection with a merger, acquisition, or sale of substantially all of its relevant assets.

Notices. Notices to Defy should be sent to info@defy.com.fj. Notices to you will be sent to the email address associated with your Defy account.

Electronic acceptance. Your electronic acceptance of these Terms (including by creating an account or clicking to accept) is legally binding to the same extent as a handwritten signature, in accordance with applicable Fijian law.