Acceptable Use Policy

Effective date: 2025

Applies To: All users of Connect3, including client organisations, administrators, and authorised end users.

Connect3 is provided by **THREEDIGITAL** to enable secure, automated data exchange between client management and finance systems. This Acceptable Use Policy ("Policy") ensures all users operate the platform responsibly, lawfully, and in a way that maintains the reliability and integrity of the Connect3 environment. By accessing or using Connect3, users agree to comply with this Policy and all related agreements, including the Connect3 Master Services Agreement and Privacy Policy.

1 Purpose

This Policy outlines the standards of use for Connect3. Its purpose is to maintain the performance, security, and stability of the platform, ensure compliance with legal and contractual obligations, promote fair use across all clients, and protect THREEDIGITAL, its clients, and users from misuse, data breaches, and disruption.

2 Fair Use

Connect3 is licensed based on fair and reasonable use in accordance with the subscription level purchased. Excessive or abnormal system activity that materially impacts service performance for other clients may be restricted or suspended at THREEDIGITAL's discretion. Examples of excessive or unfair use include attempting to bypass rate limits or usage thresholds, generating an unusually high volume of automated requests or data transactions not aligned with the subscribed plan, or repeatedly creating or deleting large data sets that cause undue strain on system resources. THREEDIGITAL will notify clients if usage patterns exceed fair use expectations and may propose a higher-tier plan if ongoing increased usage is required.

3 Prohibited Activities

Users must not use Connect3 (or allow it to be used) to upload, transmit, or process any data that is unlawful, harmful, defamatory, or infringes intellectual property rights; attempt to gain unauthorised access to Connect3 systems, databases, or other client data; test or probe Connect3 for vulnerabilities without prior written consent from THREEDIGITAL; disable, damage, interfere with, or attempt to circumvent security controls or usage limits; modify, copy, reproduce, or create derivative works from Connect3 or its components; reverse engineer, decompile, or disassemble any part of the software; use Connect3 in a way that violates applicable laws, including privacy, data protection, or export control laws; share user credentials or allow unauthorised persons to access the platform; misrepresent identity or impersonate another person or organisation; introduce viruses, malware, or malicious code into Connect3 or any connected systems; or use Connect3 to process or store data unrelated to the organisation's legitimate business operations.

4 Data and Security Obligations

Clients must ensure that data uploaded or transferred through Connect3 is accurate, lawful, and authorised for processing. Each client organisation is responsible for managing its own users, permissions, and access controls within Connect3. Clients must maintain the confidentiality of user credentials and immediately notify THREEDIGITAL of any suspected unauthorised access or security breach. THREEDIGITAL reserves the right to monitor system activity to ensure compliance with this Policy and protect the integrity of its services.

5 Compliance and Enforcement

THREEDIGITAL may take any of the following actions if a breach or misuse is detected: issue a written warning or request to remedy the breach, temporarily suspend access to the Connect3 platform, restrict specific functionality or user accounts, terminate the client's subscription or contract under the terms of the Master Services Agreement, or report unlawful activities to relevant authorities where required by law. Repeated or serious violations may result in permanent suspension of access and potential legal action.

6 Client Responsibility

Each client organisation is responsible for ensuring all users within its control comply with this Policy. Failure to enforce proper use by internal users or contractors may be treated as a breach by the client itself.

7 Reporting Misuse

Suspected misuse or security concerns should be reported to THREEDIGITAL immediately at [insert support email]. Reports will be reviewed promptly, and appropriate action will be taken to ensure the ongoing security of the Connect3 environment.

8 Updates to this Policy

THREEDIGITAL may update this Policy from time to time to reflect changes in technology, law, or business practices. The current version will always be available on THREEDIGITAL's website. Continued use of Connect3 after publication of an updated Policy constitutes acceptance of the new terms.

9 Contact

For questions about this Policy or its interpretation, please contact:
THREEDIGITAL
PO Box 634, Banora Point NSW 2486, Australia
Email: hello@threedigital.com.au