Acceptable Use Policy

Effective date: 15 November 2026

This Acceptable Use Policy (?AUP?) governs your use of Impact365 (the ?Service?) and forms part of the Terms of Service. It exists to protect the Service, our customers and third parties. By using the Service you agree not to engage in any of the activities below.

1. Prohibited activities

? Using the Service in violation of any applicable law or regulation, including the PDPA, anti-money-laundering, tax or companies legislation.
? Uploading or transmitting content that is unlawful, fraudulent, defamatory, infringing or that you have no right to use.
? Misrepresenting financial records or using the Service to facilitate fraud, tax evasion or money laundering.
? Infringing the intellectual-property or privacy rights of others.

2. Security & integrity

? Attempting to gain unauthorised access to the Service, other tenants? data, or related systems.
? Probing, scanning or testing the vulnerability of the Service without our prior written consent.
? Introducing malware, viruses, or any harmful code.
? Circumventing authentication, access controls or tenant isolation.
? Interfering with or disrupting the integrity or performance of the Service (e.g. denial-of-service, excessive load).

3. Fair use of resources

? Do not use automated means to place unreasonable load on the Service or its APIs beyond documented limits.
? Do not resell, sublicense or provide the Service to third parties except as expressly permitted.
? API access must respect rate limits and authentication requirements.

4. AI features

Do not use the AI assistant to generate misleading financial statements, to submit statutory filings without review, or to attempt to extract another tenant?s data. AI outputs are drafts for human review and are not professional advice.

5. Your responsibility for users & content

You are responsible for your users? compliance with this AUP and for the lawfulness of the data you upload, including having a lawful basis to process personal data of your employees, directors and customers.

6. Reporting

Report suspected violations or security issues to raychung@slvgroup.com.my.

7. Enforcement

We may investigate suspected violations and may suspend or terminate access, remove offending content, or report to authorities where appropriate. We will use reasonable efforts to notify you unless prohibited or where doing so could compromise security or an investigation.