



ACCEPTABLE USE POLICY (AUP)

Version: 2
Date: July 2026

1. PURPOSE AND SCOPE

- 1.1 This Acceptable Use Policy ("AUP") sets out the rules and guidelines for the use of managed services ("Services") provided by Amicus ITS Limited t/a Aura Technology ("the Company") to the Customer, as defined in the Order Form and governed by the General Terms & Conditions and relevant Service Level Agreement Schedule. The AUP applies to all Authorised Users, Devices, Services and Contacts as defined in the Order Form.

2. GENERAL PRINCIPLES

- 2.1 The Customer and its Authorised Users must use the Services in accordance with the Agreement, this AUP, and all applicable laws and regulations.
- 2.2 The Customer is responsible for ensuring that all use of the Services by its personnel, agents, and third parties complies with this AUP.
- 2.3 The Company may update this AUP from time to time. The latest version will be available at <https://auratechnology.com/terms/aup>

3. ACCEPTABLE USE

- 3.1 The following activities are strictly prohibited:
- 3.2 Storing, distributing, or transmitting any material that is unlawful, harmful, threatening, defamatory, obscene, or infringes any third party's intellectual property or other rights.
- 3.3 Facilitating illegal activity, promoting unlawful violence, or engaging in discriminatory behaviour.
- 3.4 Introducing or transmitting viruses, malware, or any device intended to impair the operation of any network, system, or data.
- 3.5 Attempting to gain unauthorised access to any part of the Company's or third-party systems.
- 3.6 Using the Services in a manner that could damage, disable, overburden, or impair the Company's infrastructure or interfere with other users' use of the Services.

4. CUSTOMER RESPONSIBILITIES

- 4.1 The Customer must maintain valid and current licences for all software used on Authorised Devices and Users.
- 4.2 The Customer must provide accurate and timely information to the Company and respond promptly to requests for information or authorisation.
- 4.3 The Customer must ensure that all devices requiring backup are authorised and backup requirements are provided to the Company.
- 4.4 The Customer is responsible for the security and management of its own systems and data, including compliance with data protection laws.
- 4.5 The Customer must not assign tasks to Company resources outside the defined scope of the Managed Service.

5. OVERUSE OF SERVICES

- 5.1 **Definition of Overuse**
- 5.2 Overuse occurs when the Customer's use of the Services exceeds the agreed scope, capacity, or reasonable usage levels as set out in the Order Form, Service Schedule, or as reasonably determined by the Company. This includes, but is not limited to:
- 5.2.1 Exceeding the number of Authorised Users, Devices, or Services without prior agreement.
 - 5.2.2 Generating excessive support tickets, incidents, or requests that surpass the agreed thresholds or the capacity of dedicated resources.
 - 5.2.3 Repeatedly requesting support for issues arising from the Customer's failure to implement the Company's recommendations, advice, or proposed projects.

6. USAGE LIMITS

- 6.1 **Support Requests:** The Customer should not consistently exceed the average monthly ticket volume or incident rate or the capacity of the dedicated resource if specified in the Order Form. If ticket volumes regularly surpass these thresholds, the Company may recommend additional resources or review the scope of service.
- 6.2 **Authorised Users/Devices:** The number of supported users and devices must not exceed those agreed in the contract. Any increase must be approved and may incur additional charges.
- 6.3 **Project and Change Requests:** Requests for work outside the standard managed service (e.g., major upgrades, migrations, or projects) will be treated as chargeable projects and are not included in the standard service.

7. CONSEQUENCES OF OVERUSE

- 7.1 If the Customer's overuse is due to not following the Company's recommendations or advice (e.g., not implementing security upgrades, ignoring technical advice, or postponing recommended projects), all related investigation, resolution, and support work will be considered chargeable at the Company's prevailing rates.
- 7.2 The Company reserves the right to suspend SLA targets if the volume of work exceeds the capacity of the shared service desk or dedicated resources, especially where recommendations have not been implemented.
- 7.3 The Company may escalate excessive or out-of-scope requests to the Authorised Contact and decline execution until a formal change request is approved.
- 7.4 The Company may suspend or limit access to the Services if overuse threatens the stability or security of the managed environment.

8. COMPLIANCE AND ENFORCEMENT

- 8.1 The Company reserves the right to monitor usage and enforce this AUP. Breaches may result in suspension or termination of Services, and the Customer may be liable for any costs, losses, or damages arising from non-compliance.
- 8.2 The Customer is responsible for any charges incurred because of overuse, unauthorised activities, or failure to follow recommendations.

9. REVIEW AND UPDATES

- 9.1 This AUP will be reviewed periodically and updated as necessary via the Company's website. Customers will be notified of material changes in writing.