

## About this document

This is a description of how the Enate Solution is hosted to make it available in the form of software-as-a-service. It applies to contracts that incorporate this document by reference. It will be updated from time to time, and revised versions will be published at the same location online. If you want to be notified about changes, please email [contracts@enate.net](mailto:contracts@enate.net) and provide your name, the name of your organisation (which must match the name of the organisation that has a contract with us), your role, and say that you want to subscribe for change notices regarding Hosting the Enate Solution – The Enate Platform. Look out for an acknowledgement of your request.

## Hosting the Enate Solution – the Enate Platform

The Enate Solution supplied as software-as-a-service is hosted on a platform called the ‘Enate Platform’.

### Delivering the Enate Platform

Enate shall:

- install, configure and operate the Enate Solution in accordance with good industry practice;
- perform all administration on the platform including configuration of plugins and integrations that are designed to be deployed by platform administrators. These include user data stores, integration adapters, installation of the platform plugins, configuration of password policies, and configuration of platform level defaults;
- provide and manage all server-side hardware and operating systems relating to the delivery of the Enate Solution, including servers and communication equipment, within a secure environment (described below); and
- provide the Enate Platform to meet the service levels described within Maintenance & Support (<https://docs.enate.net/enate-contract-documents/>).

### Security of the Enate Platform

The security of the Enate Platform will always be managed within the scope of Enate’s ISO27001 accredited information security management system. Enate shall:

- Manage the platform in line with the ISO27001 information security management system as set out in documents maintained as ‘ISMS 024 – *Enate Statement of Applicability and ISMS 025 - Enate Where is My Data and How is it Stored and Protected*’ which will be kept up to date. This document can be found at <https://docs.enate.net/enate-contract-documents/>.
- Provide the Enate Platform such that Customer Data is logically separated from any other customer’s data
- Manage and install changes, new version updates or patches to operating systems, the application or hardware
- Provide and manage firewall security and intrusion detection systems to restrict access and block unnecessary ports
- Install and maintain anti-malware on all servers
- Give reasonable access and support to Customer as required to perform regular vulnerability scanning and penetration testing provided that such testing is performed against the internet-facing surface of the Enate Solution
- In the event of a security breach, allow Customer monitored access to servers in order to conduct forensic imaging of said servers

Updates are described in more detail within Maintenance & Support (<https://docs.enate.net/enate-contract-documents/>).

### Platform Maintenance

From time to time it is necessary to perform maintenance on the Enate Platform to ensure continued smooth operation and optimised performance. For planned maintenance, Enate will always provide five working days notice which will then normally take place on a weekend. Enate strive to conduct maintenance without the need for downtime on the platform, but in cases where this not possible, Enate will provide notice and approximate details of the downtime window to affected customers.