Operator FAQ

essensys Operate

1. How does essensys keep my business safe from security threats?

essensys platforms are regularly audited by independent security professionals. essensys Operate was last audited in December 2016, with all findings remedied.

essensys recognises the importance of data stored on the platform. Only authorised operator end-users have access to that data, with no ability for data to be accessed by un-authorised users.

essensys platforms are hosted in data centres with ISO 27001 and PCI DSS accreditation.

essensys constantly monitors and audits its access rules and policies, and grant access only as required by both software and users. Latest OS and software patches are regularly applied.

2. What anti-virus & anti-malware protection is provided? What other security measures are in place?

Windows Defender, now a standard part of Windows Server 2016, runs on all machines involved in running Operate software. No additional software is being installed on any of the machines, keeping the attack surface negligible and fully manageable.

3. Where is Operate data stored and does UK data protection laws apply, if not what laws are applicable?

essensys Operate data is stored in the European Union, in the Republic of Ireland. Section 9 of the essensys terms and conditions (available here: https://essensys.tech/our-terms) provides details of essensys data protection. For the purposes of the UK Data Protection Act (1998), the data controller is essensys Limited.

4. In the event of essensys company difficulties, what assurances are provided to safeguard my data and access to that data?

Section 5.3.1 of the essensys terms and conditions (available here: https://essensys.tech/our- terms) ensure that the operator can terminate the agreement if essensys ceases or threatens to cease to carry on business. The operator's data is safeguarded in in line with section 5.6 of the terms and conditions.

5. Does the standard contract explicitly state the ownership rights of the operator with regard to the data stored within the essensys platform?

Section 4.2 of the essensys terms and conditions (available here: https://essensys.tech/our-terms) ensures that the operator has sole ownership rights for all of the operator's data.

6. In the event of a termination of contract, what measures are in place to securely remove and dispose of operator data?

Section 5.6 of the essensys terms and conditions (available here: https://essensys.tech/our-terms) ensures continuation of our data protection policy in the event of termination of contract. Section 5.8 of these terms and conditions ensures that data is securely removed, and, if required, returned to the operator.

7. What backup policies are in place, how often is data backed up? Is it differential based or complete backup copies?

Backups are performed once overnight, every night. These are full backups.

8. What are the timescales for data restore requests?

Data that users delete is sent to a recycle bin section within the product which users can restore themselves.

If restoring from a backup, usually 20 minutes are enough for the team to restore the database, however this depends heavily on the size of the database.

9. How long does an actual restore procedure take?

This is typically instant but will depend on how much data is being restored.

10. What are the daily hours for system support? Is weekend support included?

The essensys platform is proactively supported 24 hours a day, 365 days a year. essensys can be contacted for system support from Monday to Friday from 08:30 am to 01:30 am (the next day). essensys can be contacted outside of these hours for critical system issues.

11. Does essensys undergo independent security audits? Is there a results history available?

essensys platforms are regularly audited by independent security professionals. essensys Operate was lasted audited in December 2016, with all findings remedied. These results are not made available to customers.

12. What are the disaster recovery plans for the essensys platform?

essensys platforms are established with full data resiliency, and are not dependant on essensys offices being "open-for-business". Should a data centre fail, essensys disaster recovery plans ensure we have an operating capability to provide service continuity via standby platforms. To support the platform, essensys can deliver the full support capability from distributed UK locations, and from our premises in the United States.

13. What level of disaster recovery liability is accepted by essensys in respect of lost or stolen operator data or as a result of a prolongedoutage?

essensys is able to restore data from backups if required to protect against data loss. Prolonged outages are minimised via our disaster recovery plans.

14. Does the liability clause ensure that essensys will and must allow for a third party to perform a root cause analysis and be bound by thefindings?

essensys does not employ a third party to perform incident root cause analysis. essensys is, however, dependant on our suppliers and third-party partners to perform root cause analysis on incidents for services essensys depends on to provide solutions to the operator. Findings and recommendation from this analysis are followed through by both essensys and our suppliers / partners.

15. What bandwidth is available to the hosted servers, both the primary and disaster recovery locations?

Adequate bandwidth is provided to the servers to handle use. Bandwidth is adjusted as is seen necessary.

16. How many concurrent users is the system designed to facilitate and what are the expansion plans for user growth as the essensys client base expands?

essensys have a dedicated Dev Ops and platform team who monitor our platforms for performance and capacity and perform upgrades whenever it is perceived necessary to maintain a healthy system. This includes any necessary scaling plans to handle a growing user base.

17. What system performance management exists and is this information available to us and at what periods?

As above, our teams use a range of tools and processes to monitor performance and adjust platforms as required. This data is not shared with customers.

18. Have essenys quantified the additional system load requirements for concurrent billing procedures and invoice runs by multiple clients on a single day?

Our teams monitor load requirements based on historical, current and predicted use.

19. What if any, performance degradation occurs for users on billing day? How is this being addressed?

Performance of the platform is not impacted when clients perform bill runs

20. Are there plans to improve this? Is average system response time monitored and when is the information made available toclients?

The parts of the platform and application which require it are monitored for performance and responsiveness. If it is felt and area of the system is failing against its benchmarks then corrective action is taken to rectify this. This information is currently not shared with clients.

21. What annual planned system outages/downtime is required in respect of the essensys platform?

There are no annually planned system outages for essensys Operate.

22. How far in advance are system upgrades notified to clients together with the provision of detailed specifications of the planned upgrades?

Any system (platform) upgrades happen behind the scenes and are not client facing. Enhancements to the software are announced as they are released. If any fundamental changes to the software are due to take place which may drastically alter how clients use the software then typically 2-4 weeks' notice is provided.

23. What are the timescales involved for upgrade rollbacks?

If a software release takes place that requires a rollback (very rare) then this happens instantly.

24. How often are upgrades released?

Software releases typically happen twice a week

25. On which day(s) and at what time(s) are upgrades implemented?

This varies depending on the type of the release