

IMDEX HUB-IQ™

Information Security



IMDEX understands the importance of the security and safety of your data. For over ten years we have been managing data for some of the largest companies in the world in our cloud. For this reason we use ISO27001 certified and globally recognised cloud service providers to ensure information security. We also employ a team of IT professionals globally so you can have confidence in your data.

Independently verified services ensure compliance for all infrastructure and applications in IMDEXHUB-IQ™. Our regular audit and compliance reports provide insights and ensure specific regulatory standards are always met.

How do I know my information is secure in the cloud?



- IMDEX's information and communication technology (ICT) infrastructure undergoes annual third-party penetration testing
- IMDEX employs an in-house certified cloud security professional (ISC2) to assess the cloud environment on a continuous basis
- IMDEX has an information security strategy aligned with CIS20
- Development of the source code follows DevSecOps principles and internal developers receive annual DevSecOps training.

How does this work?



Technology safeguards such as encryption, and operational processes around data destruction keeps your data safe.

- Encryption is used to secure your data in-transit and at-rest
- Role based access control is supported using application specific means
- Service level agreements (SLA) between cloud service provider and IMDEX ensures availability of your services.

Who has access to my data?



- Your data privacy is a priority
- Our offer is Software as a Service (SaaS), so on a day to day basis, your data is managed by only you
- Access is strictly controlled with permissions. Access is controlled on request as necessary, to provide or troubleshoot the service. Only our IMDEXHUB-IQ™ support team are allowed access to client data and sign stringent confidentiality agreements restricting them from sharing data even with other staff members
- Client data is segregated through logical separation and access is controlled based on the tenant ID.

How is my data protected against current and emerging threats?



- ICT systems are scanned using vulnerability management tools
- Next-gen firewalls with zero-day protection capabilities are used for perimeter defences

Regulatory compliance

- IMDEX has a cyber security incident response plan encompassing OAIC (Office of Australian Information Commissioner) mandatory data breach notification scheme
- IMDEX procedures are being aligned with the European Union's GDPR (General Data Protection Regulation).
- IMDEX conducts due diligence on all ICT suppliers and gives preference to suppliers compliant with ISO27001.



Data availability and backups

We routinely perform backups that are held separately from the main database.



- We have a disaster recovery procedure and backup regularly to a separate disaster recovery (DR) site located at a geographically separate location
- We have 99.95% availability – and list the recovery point objectives (RPO) and recovery time objectives (RTO) in our security document
- A recovery procedure is in place describing the process required to restore the system from a failure
- Appropriate support agreements are in place for all components in order to achieve availability targets.

