

# Information Security Policy

We will establish, maintain, and continually improve an ISMS (information security management system) to manage the risks facing information belonging to databasics and relevant interested parties. We aim to protect that information from all threats (whether internal or external, deliberate, or accidental), and safeguard its confidentiality, integrity, and availability. Specifically, we will ensure that:

- Business requirements for the availability of information and information systems are met.
- Information will be protected against unauthorised access.
- Confidentiality of information will be assured, by protection from unauthorised disclosure, theft, or intelligible interruption.
- Integrity of information (its accuracy and completeness) will be maintained by protecting against unauthorised modification.
- Regulatory and legislative requirements will be met.
- Business Continuity plans will be produced, maintained, and tested, to ensure that information and vital services remain available in the face of adverse events.
- Information on security matters will be made available to all employees and relevant contractors.
- All breaches of information security will be reported to the CISO and investigated appropriately.
- A suitable program of independent review is implemented to identify any weaknesses in the implementation of technical security controls on classified assets.
- Our ISMS is established and maintained in compliance with the ISO 27001 standard.

# databasics

While the CISO and team play a key role in administering our ISMS, it is the responsibility of all everyone working for our organisation to adhere to the Policy.



Ricky Patten  
business owner and CISO  
5th June 2023