

Civica's commitment to security

At Civica we're committed to operating and maintaining a secure environment and we've implemented the policies, procedures, tools, and technologies to comply with the internationally recognised ISO27001 and ISO22301 standards, Cyber Essentials (UK) and Essential Eight (Australia) to ensure the confidentiality, integrity, and availability of our information and systems.

We use comprehensive security monitoring tools, develop code securely from the outset, and regularly test our approach with targeted security testing. This includes regularly testing the processes designed to keep data secure from unauthorised access or changes, and the measures in place to defend Civica products and networks from cyber-attacks.

Civica is committed to ensuring:

- Personal data of customers, citizens, and employees are protected
- Individuals' privacy rights are upheld
- Legal, contractual, and regulatory requirements are met
- Ongoing compliance with and certification to the standards listed above
- Confidentiality, integrity, and availability of information is maintained
- Information security and privacy risks are identified and managed
- Business continuity plans are maintained and tested
- Suspected breaches of information security and privacy are reported, investigated and actions taken to avoid recurrence
- Other security controls such as PCI-DSS are appropriately applied where applicable.

Security measures are generally aligned with the ISO27001 standard and govern all areas of security including physical access, system access, data access, transmission, input, security oversight, and enforcement.

Civica implement and maintain:

- 1) Organisational management processes, security controls and policies which are reviewed and approved by executive leadership.
- 2) Security controls that include logical segregation of data, restricted (e.g. role-based) access and monitoring. User account access is revoked upon termination of employment.
- 3) Industry best practice encryption to protect personal data and any other sensitive data at rest and in transit.
- 4) Access controls designed to manage electronic access to data and system functionality based on authority levels and job roles. A least privilege approach is taken so that access to information and services is denied by default.
- 5) User IDs and password configuration requirements that are designed to uniquely authenticate users and ensure the principle of non-repudiation is maintained.
- 6) Facilities, data centres and cloud providers that provide appropriate assurances that they have security controls available that align to these Security Measures.
- 7) Operational procedures that are designed with security in mind and monitored to ensure they achieve security objectives.

- 8) A change management process to ensure that systems remain secure and resilient.
- 9) An incident response plan to ensure minimum business impact in the event of a disruptive event.
- 10) Network connections into and out of Civica services which are controlled by appropriately designed and implemented network security measures and in line with our security policies.
- 11) Vulnerability assessment, threat protection technologies, and scheduled monitoring procedures which are designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.
- 12) Business continuity and disaster recovery procedures aligned to the ISO22301 standard that ensure service and recovery from emergency situations or disasters.
- 13) Periodic audit procedures for the purposes of review and assessment of security risks, monitoring compliance with Civica's policies and procedures, and reporting the condition of its information security and compliance to management.