Information Security at Civica

As a global GovTech provider, Civica have a strong track record around systems and data integrity. We continuously review and improve our software, systems, and processes in accordance with industry best practice, and utilising advice and threat information from specialist security organisations, such as the National Cyber Security Centre (NCSC).

We maintain an information management system underpinned by technical and organisational controls accredited against globally recognised standards including ISO 27001 (information security), ISO 22301 (business continuity), and Cyber Security Essentials.

Civica continually improve our practices to maintain our high standards and provide our customers and colleagues the assurance that security and resilience are – and will always remain – our number one priority as a company.

Civica's Commitment to Data Security & Privacy

Civica is committed to ensuring:

- Personal data of customers, citizens, and employees is protected.
- Individuals' privacy rights are upheld.
- Legal, contractual, and regulatory requirements are met.
- Ongoing compliance with, and certification to, a range of international standards.
- Confidentiality, integrity, and availability of information are 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 and investigated, and appropriate actions are taken to avoid recurrence.
- Other security controls such as PCI-DSS are appropriately applied and certified against.

How Civica Protects Customer Data

Outlined below are some of the key steps we take, as standard, to ensure we deliver the highest levels of protection across customer solutions.

Management Framework

Series of policies, procedures, and controls that are in place to maintain IS and DP…

Civica is currently certified to ISO 27001, ISO 22301, and the UK's Cyber Security Essentials standards.

In line with these certifications, organisational management policies, procedures, and security controls are reviewed and approved by executive leadership as part of our information security and data privacy programs (ISMS/PIMS)

Audit

Civica has a comprehensive audit program for monitoring compliance with our policies and procedures. Performance against information security and privacy objectives is reported to senior management on an ongoing basis.

Independent verification by UKAS-accredited auditors of Civica's security controls and practices is a vital part of our approach to governance and occurs on an annual basis.

Product Security

Product teams across Civica apply a consistent approach to secure software development, and embed privacy by design and by default. We verify the security of our products through a comprehensive ongoing assessment process, consisting of extensive vulnerability scanning, secure code testing, and penetration testing.

A comprehensive change management process is also applied to ensure that systems remain secure and resilient.

Credential and authentication configuration is in place across our products which is designed to uniquely authenticate users and ensure the principle of non-repudiation is maintained.

Civica uses industry best practice encryption to protect personal data and any other sensitive data at rest and in transit.

Operations

Monitoring & Testing

We utilise vulnerability assessments, threat protection technologies, and scheduled monitoring procedures which are designed to identify, assess, mitigate, and protect against security threats, malware, and other malicious activity.

Our in-house CREST-accredited penetration test team employ a range of technical security assessments on our operating infrastructure and platforms, the software we build and, in line with contractual requirements, on customer implementations.

The Civica Security Operations Centre (SOC) is supported by a leading 24/7 managed SIEM service which provides incident analysis, and threat hunting and intelligence.

Civica work with leading third-party providers to conduct security posture scoring and quantification to further validate our practices and provide tangible assurance to our customers.

Human Resources

All Civica personnel undergo pre-employment background checks appropriate to the nature of their role and are subject to confidentiality agreements.

To ensure all our colleagues are aware of the importance of their role in protecting data, they are supported by an ongoing education program including mandatory annual security and privacy training.

Access Control

Security access controls are used across the breadth of our operations which include logical segregation of customer data, role-based access control (RBAC), and multi-factor authentication (MFA).

A least privilege approach is taken so that access to information and services is denied by default. Data access is provided only to those who need it, and user account access is revoked upon termination of employment.

Communications Security

Network connections into and out of Civica services are controlled by appropriately designed and implemented network security measures including firewalls, IPS/IDS, and encrypted VPNs for remote workers.

Email is managed via a secure gateway with additional threat protection powered by AI.

Information is transferred using approved methods with additional protective measures.

Supplier Relationships

Civica operate a holistic third-party security programme. As such we only work with facilities, data centres, and cloud providers that provide appropriate assurances that they utilise security and privacy controls aligned to our standards.

We conduct in-depth assessments of our suppliers to review their practices and ensure the security of the data they process on our behalf. Where data is transferred to third countries, appropriate mechanisms are in place including the latest UK and EU Standard Contractual Clauses

Incident Management

Business continuity and disaster recovery procedures ensure service resilience during emergency situations or disasters.

In line with ISO 22301, incident response plans are designed, implemented, and tested regularly to ensure minimal business impact in the event of a disruptive event.

Any incident, whether a breach or a near miss, is analysed to ensure all corrective measures and improvements are identified and implemented.

Backups are regularly taken and tested and stored in geographically separate data centres to production environments.