4C STRATEGIES

Secure, Customer-first Resilience Software

Safeguarding Your Data Empowering Your Operations

As a provider to Fortune 500 companies, governments, allied forces, and international organizations, we are committed to ensuring the confidentiality integrity and availability. of our customers' data. To safeguard your data and meet your zero trust requirements, we uphold strict information security standards and follow industry best practices as part of a robust approach to data security and hosting.

Security is in our DNA

Washington D.C. | Orlando | London | Stockholm | Brisbane | Malmö | Warminster

Cloud Hosting Security

We utilize modern cloud hosting services or data centre technology with high-availability and strict security to ensure robust and reliable access to your data, 24/7.

Data Centers

Our SaaS solution is hosted in secure ISO 27001 certified data centres on robust infrastructure with load balancing capabilities in North America, Europe, and Australia.

Hosting

The 4C Resilience platform is either hosted in 4C's private cloud, or by a public cloud provider such as Microsoft Azure. The 4C private cloud infrastructure is built with multi-layered security measures, including encryption, advanced threat detection, continuous monitoring, and high-availability architecture, that safeguard your sensitive data against evolving cyber threats and ensures your business-critical data is always accessible.

Read more about infrastructure security at Azure which we use for hosting in North America and Australia.

Facility Security

Hosting facilities include redundant components for independent power, cooling, and networking, and concurrent maintainability, allowing for planned maintenance without service interruption. Physical controls include fire suppression and surveillance systems, as well as strict access approval at facility's' perimeter, buildings' perimeter and inside buildings.

Read more about facility security at Azure

Data Encryption

Data in Transit

All client data is encrypted at industry standards encryption. Data in transit is encrypted at TLS v1.2 or above as supported by clients.

Data at Rest

Data at rest is encrypted with at least AES256 encryption algorithms.

Security of Networks

Controlled Access

For private data centers access to production environments is limited to authorized personnel with a valid "need-to" operational requirement. All access is logged and utilizes multi-factor authentication for enhanced security.

Network Segmentation

Services are organized into separate trust zones based on their level of sensitivity, with minimal inter-zone traffic to reduce risk.

DDoS Attack Mitigation

Comprehensive measures are implemented to detect and manage denial-of-service (DDoS) attacks, to uphold system availability.

Application Traffic Protection

A Web Application Firewall (WAF) is in place to shield incoming traffic from vulnerabilities, including threats such as SQL injection and cross-site scripting (XSS).

Availability & Continuity

Operational Oversight

We continuously monitor essential service metrics and server logs to identify, prevent, and respond to potential service disruptions.

Redundancy

Hosted data is securely replicated between regions or datacentres ensuring high-availability and rapid recovery in any crisis scenario.

Service Availability Updates

4C provides real-time updates on scheduled maintenance and service disruptions to designated customer Points of Contact using agreed channels.

Business Continuity

As a provider of Continuity software and services we have comprehensive plans and processes in place to manage major disruptions and emergency events. Our plans are regularly tested and updated to ensure effectiveness.

Data Backup & Retention

Data is automatically backed up every 24 hours and stored for a minimum of 3 months, with an option to extend retention to 365 days. Backups are moved to safe storage using either offline or immutable functionality.

Identity & Access Management

Our IAM processes ensure only authenticated and authorized users can access data in the application while delivering nonrepudiation for application and system actions.

Data Centers

Our SaaS solution is hosted in secure ISO 27001 certified data centres on robust infrastructure with load balancing capabilities in North America, Europe, and Australia.

Authentication

Our software supports Single Sign-On (SSO) with Multi Factor Authentication (MFA) integrations with OpenID compliant identity providers including EntraID (formerly known as Azure AD). Multi-factor authentication is supported using either an included Keycloak IAM service or a third-party identity provider. Our software also supports standard username/password authentication.

Authorization

Granular role-based access controls can be set according to entity and attributes through associated groups and roles. For more complex authorization scenarios, runtime dynamic access permissions can be applied.

Development and Application Security

4C implements robust security practices across its development process and vulnerability management to ensure our software remains secure and resilient against evolving threats.

Secure development

Security-Focused Development
Our development lifecycle incorporates rigorous information security protocols, with comprehensive risk assessments and structured change control procedures.

Developer Security Training
Developers receive training in secure coding practices, including the OWASP Top 10 vulnerabilities.

Isolated Testing Environments
Development and testing activities are carried out in isolated environments, utilizing non-production data to ensure separation from live systems.

Vulnerability Scanning
All source code undergoes vulnerability testing to ensure no code is deployed until any identified issues are resolved.

Restricted Production environments
Access to production environments is strictly limited to authorized personnel based on operational necessity. Multi-factor authentication is required for all access.

Proactive Vulnerability Management

Regular Penetration Testing
Our application undergoes annual penetration tests by a third party with an emphasis on OWASP Top 10 security risks against web applications. This ensures only authenticated and authorized users can access data in the application while ensuring nonrepudiation for actions in our application and underlying systems.

Organizational Information Security

People have a key role to play in upholding security therefore we have comprehensive processes in place to ensure security is not compromised.

Internal

IT Service Access Control
Access to 4C's essential IT services is managed centrally and supported by multi-factor authentication. Only compliant company devices are permitted to access critical services.

Device Protection
All company devices are required to have encryption, up-to-date end-point protection software, and active firewalls to meet strict security requirements.

Incident Response & Management

Incident Response
As a provider of incident and crisis management software and service we have robust response processes in place. We train relevant staff in effective security incident response procedures, including communication channels and escalation paths. In case of a major incident, responders are backed by our crisis management team.

Supplier Management
We maintain a detailed register of all providers involved in service delivery, and regularly review the security posture of critical vendors. No data is shared with third parties for any other purpose then delivering the services we provide.

Human Resources & Security

Principle of Least Privilege
We work according to the principle of least privilege. Any access to customer data is on a need-to-know basis and requires approval prior to it being granted.

Staff Training
All employees are required to complete a security training program, covering such things as cybersecurity threats, physical security, etc. when they start at the company. An annual program is run annually to ensure all staff know and follow the appropriate policies and procedures.

Company Best Practice
We uphold strict information security standards in company practices, with the appropriate policies, processes, training, and technology in place to mitigate any identified risks to our business and customer data.

Confidentiality & Legal Protections
All 4C employees are bound by non-disclosure and confidentiality agreements outlined in their employment contracts.

Privacy

Personal Data in the software

Personal Data or Personal Identifiable Information (“Personal Data”), such as names, email addresses, and login credentials, is processed in the software to facilitate the setup and management of customer user accounts. The data required in the software is limited to what is strictly necessary to provide a secure and functional user experience. The software does not request any additional data beyond what is essential for its core functionality. The customer is responsible for identifying, determining the lawful processing of, and ensuring the secure handling of any Personal Data necessary for their use of the software. If the GDPR applies, the customer is considered the data controller and is therefore responsible for the data controller obligations according to the GDPR.

Information Security

Our comprehensive security measures are outlined above, highlighting how we safeguard your data. For information on access control see the sections above.

Data Residency

For hosted solutions, the software is either hosted by 4C’s internal servers, or by a third-party hosting provider such as Microsoft Azure. For our European customers, all customer data is stored within EU/EEA. For our Australian or US customers, all customer data is stored in data centers located in Australia or the US.

Third-party Processing

4C continuously reviews its third-party suppliers to ensure that appropriate security measures are in place to safeguard Customer Data, including Personal Data, and maintain compliance with relevant regulations. Apart from the hosting provider, Microsoft Azure, 4C’s sub-processors are exclusively 4C group companies.

To ensure high availability and the best customer service possible, 4C’s support team operates within 4C’s group companies across different jurisdiction and time zones. The support team may access the software, including Personal Data processed therein, to provide remote support. However, all data remains stored in the relevant hosting location. The 4C support team only accesses Customer Data, including Personal Data, to provide support.

In accordance with GDPR, 4C has intercompany agreements in place between our group companies, including standard contractual clauses. 4C has further conducted transfer impact assessments regarding potential third country transfers.

Incident Response and Reporting

4C has established robust internal guidelines and processes for addressing potential cyber incidents that may impact Personal Data. In the event of such an incident, 4C will notify affected customers as per the notification time frame set out in the contract or without undue delay, but not later than 72 hours after becoming aware of the incident.

Request for Personal Data

In the event that 4C receives a legal request for Personal Data or an inquiry from an individual regarding their Personal Data, 4C will, unless prohibited by law, promptly inform the Customer. 4C will disclose data solely as mandated by legal requirements.

Compliance, Certifications and Accreditations

We follow guidelines and best practices in accordance with the 27001 standard for information security management system. In that respect, we have implemented comprehensive security measures, best practices and processes to protect sensitive data, mitigate cybersecurity risks, and ensure the confidentiality, integrity and availability of information.

4C STRATEGIES

4C Strategies is the leading provider of training readiness and organizational resilience software and professional services. With over 20 years of expertise, we support high-profile international institutions, global enterprises and armed forces across 100 countries. We help you to transform training, rethink risk, manage crises, and uphold continuity - so you are ready for the resilience challenges ahead.

Find Us On www.4cstrategies.com

Washington D.C. | Orlando | London | Stockholm | Brisbane | Malmö | Warminster