cXc

A TRADING NAME OF CONXCHANGE PVT LTD

EXTERNAL TRUST & SECURITY DOCUMENT

Trust & Security Overview

How cXc protects customer data and operates a resilient platform

v1.0 · Effective 01-06-2026· Classification: Public

Document	Trust & Security Overview (External)
Version	1.0
Effective Date	01-06-2026
Last Updated	01-06-2026
Classification	Public
Owner	Chief Information Security Officer, cXc
Contact	Info@mycxc.services
Review Frequency	At least annually, or on material change

1. About This Document

cXc — a trading name of conXchange Pvt Ltd — provides software-as-a-service and platform-as-a-service technology to the insurance industry. Our customers include insurers, managing general agents (MGAs), brokers, and other insurance-sector organisations operating in the United Kingdom and European Union.

This Trust & Security Overview describes, at a level appropriate for a public document, how we protect the information entrusted to us, how we operate our platform, and how we respond when something goes wrong. It is intended to give customers, prospective customers, their auditors, and their regulators the confidence they need to work with us.

More detailed information — including our full Information Security Management System documentation, penetration testing reports, audit reports, and sub-processor list — is made available to customers and their auditors under appropriate confidentiality arrangements. Contact details for specific requests are at the end of this document.

2. Our Security Commitment

We treat the information our customers entrust to us, and the personal data of the individuals our customers serve, as something we are accountable for — not merely something we hold. That accountability shapes how we design our services, how we run our operations, and how we invest our engineering effort.

Our commitments are practical rather than aspirational:

- We operate an Information Security Management System aligned with ISO/IEC 27001:2022, covering the full lifecycle of our services.
- We host exclusively on Microsoft Azure, in UK and EU regions, with data residency commitments appropriate to the data being processed.
- We encrypt personal and confidential data at rest and in transit, using industry-standard cryptography.
- We apply the principle of least privilege, multi-factor authentication, and just-in-time privileged access across our production environments.
- We maintain documented plans for incident response, business continuity, and disaster recovery — and we test them.
- We hold our suppliers and sub-processors to equivalent standards, with contractual flow-downs and ongoing oversight.
- We are transparent with customers and regulators. When something goes wrong, we say so, promptly and specifically.

3. Governance and Certifications

Information security at cXc is owned by the Chief Information Security Officer and governed through the Information Security Steering Group, which meets monthly and reports to the Executive Committee and the Board. Our Data Protection Lead provides dedicated privacy oversight and serves as the primary contact for data protection matters.

3.1 Certifications and Alignment

Framework	Status	Notes
ISO/IEC 27001:2022	Planned	ISMS covers all in-scope services, environments, and personnel
ISO/IEC 27017 & 27018	Aligned	Cloud-specific controls and PII-in-cloud protections
ISO/IEC 27701	Aligned	Privacy Information Management extension
UK GDPR & EU GDPR	Compliant	Separate Privacy Notice published
Solvency II outsourcing	Aligned	Article 49 / EIOPA Cloud Outsourcing Guidelines
DORA (Regulation (EU) 2022/2554)	Aligned	ICT third-party provisions built into customer contracts
NIS 2 Directive	Aligned where applicable	Reviewed against essential / important entity criteria
SOC 2 Type II	Planned	Trust Services Criteria — Security, Availability, Confidentiality

Evidence on Request

Certification letters, Statements of Applicability, audit reports, penetration-test summaries, and our full sub-processor list are made available to customers and

> prospective customers under NDA. Request through your account contact or info@mycxc.services.

3.2 Supervisory Authority Engagement

We cooperate with the UK Information Commissioner's Office, with relevant EU data protection supervisory authorities, and — through our regulated customers — with their prudential and conduct regulators. Where a customer's regulator exercises the audit and access rights set out in their contract with us, we support those rights.

4. Platform Architecture and Data Residency

4.1 Hosting

cXc is built on Microsoft Azure. We use Azure services exclusively for our production infrastructure. We do not operate our own data centres and we do not use servers hosted in private premises, coffee-shop Wi-Fi, or developer laptops to run production workloads.

Our default production regions are UK South (primary) and UK West (secondary) for UK customers, and West Europe and North Europe for EU customers. Customers may contract for specific regional arrangements where their regulatory or commercial position requires it.

4.2 Data Residency

Personal data processed through the cXc platform is pinned to the Azure region selected for the relevant customer tenant. We do not route customer personal data through non-UK / non-EEA regions except under a lawful transfer mechanism agreed with the customer and subject to appropriate safeguards (see our Privacy Notice and the Data Processing Agreement).

Microsoft Azure's EU Data Boundary commitments further limit where customer data and support data may flow; we align our configuration with those commitments where applicable.

4.3 Tenant Isolation

Customer tenants are logically isolated. Access-control, row-level scoping, and identity-aware data-plane enforcement are tested as part of our secure development process. We do not run shared infrastructure patterns in which one customer's processing could, through a configuration error alone, expose another's data.

5. Data Protection

5.1 Encryption

We apply encryption in depth:

- Data in transit is encrypted using TLS 1.2 as a minimum, TLS 1.3 where supported end-to-end.
- Data at rest is encrypted using AES-256 or equivalent, with keys managed in Azure Key Vault.
- Customer-Managed Keys are available for customers whose regulatory or contractual position requires them.
- Bring-Your-Own-Key arrangements are supported under contract.
- Cryptographic choices are reviewed periodically against current industry guidance and, where applicable, post-quantum readiness planning.

5.2 Access Control

Access to customer environments and customer data is governed by the principle of least privilege. Specifically:

- Every user, whether customer, staff, or third-party, has a named identity. Shared accounts are prohibited in production.
- Multi-factor authentication is enforced on all access to internal administrative systems. Customer tenants are configured to require MFA by default, and single sign-on is offered where the customer's identity provider supports it.
- Privileged access to production is granted just-in-time, through Microsoft Entra Privileged Identity Management, with time-bound activation, ticket references, and, for sensitive roles, two-person approval.
- Break-glass accounts exist, are sealed, and are monitored. Any use is alerted in real time.
- Access reviews are conducted on a defined cadence — quarterly for privileged and customer-data access, semi-annually for standard access.

5.3 Data Classification and Handling

We classify information as Public, Internal, Confidential, or Restricted, and apply handling rules proportionate to each level. All personal data is treated as Confidential or higher. Special category personal data (Article 9 UK/EU GDPR) and criminal-conviction data (Article 10) are treated as Restricted, with correspondingly tighter controls on access, logging, retention, and transfer.

5.4 Personal Data

How we process personal data — the lawful bases, data subject rights, international transfer mechanisms, retention periods, and contact points — is set out in our Privacy Notice, which is published on our website alongside this document.

6. Secure Software Development

6.1 Development Lifecycle

Security is integrated into the software development lifecycle rather than treated as a final review step. Our standard practice includes:

- Threat modelling for new features handling personal data, financial data, or operational control surfaces.
- Peer review on every code change to protected branches, with required reviewers and required status checks.
- Automated security testing in CI — dependency scanning, static application security testing (SAST), secret scanning, and infrastructure-as-code policy checks.
- Separation of development, test, and production environments. Production data is not used in development or test except under controlled and approved circumstances.
- Change management with documented approval, rollback procedures, and post-deployment verification.

6.2 Test Data

Where test data needs to approximate production characteristics, we use synthetic data, anonymised data, or pseudonymised data rather than live customer records. Where anonymisation is used, we apply it in line with ICO and EDPB guidance on what constitutes effective anonymisation under UK/EU GDPR. Use of live customer data in non-production environments is restricted and logged.

6.3 Supply Chain

Open-source dependencies are managed through automated software composition analysis. A Software Bill of Materials is produced for each production release. Dependencies with known critical vulnerabilities are escalated and remediated within defined timeframes (see Section 7.2). Build infrastructure and CI/CD pipelines are treated as sensitive internal systems with commensurate controls.

7. Operational Security

7.1 Change Management

Production changes follow a documented change-management process. Each change has a named owner, a documented purpose, peer review, test evidence, and, where applicable, a rollback plan. Emergency changes — those required to resolve an active incident or security issue — follow an abbreviated process with retrospective documentation and review.

7.2 Vulnerability Management

We scan our infrastructure and applications continuously. Vulnerabilities are triaged and remediated against published internal SLAs, summarised below for customer visibility:

Severity (CVSS)	Remediation Target
Critical (9.0–10.0)	Within 7 days of identification
High (7.0–8.9)	Within 30 days
Medium (4.0–6.9)	Within 90 days
Low (< 4.0)	Risk-based prioritisation

Where a vulnerability cannot be remediated within the target timeframe, we apply compensating controls, document an exception, and track it to closure. Exceptions are reviewed at the monthly Information Security Steering Group.

7.3 Security Testing

Our testing programme includes:

- Continuous automated vulnerability scanning of production and pre-production environments.
- Annual third-party penetration testing of the platform and, where relevant, specific customer-requested engagements on a cost-recovery basis.

- Red team exercises on a cadence proportionate to risk and regulatory expectation (including DORA Threat-Led Penetration Testing where applicable to in-scope customers).
- A published Vulnerability Disclosure Policy and coordinated reporting channel for external security researchers — see https://www.cxc.services/security.

Findings are tracked through to remediation. Summaries of results and remediation progress are made available to customers under appropriate confidentiality.

7.4 Logging and Monitoring

We log authentication events, administrative actions, access to sensitive data, and application audit events. Logs are collected to a central Security Information and Event Management system, retained for a minimum of twelve months online and longer in archive, protected against tampering, and monitored for defined anomaly patterns. Clocks are synchronised to an authoritative time source across the estate to ensure log integrity and cross-system correlation.

7.5 Malware and Endpoint Protection

All corporate endpoints run managed endpoint protection with modern detection and response capability. Endpoints are enrolled in mobile device management, required to be compliant (encryption, patch level, active protection) before accessing Internal or above data, and monitored for policy drift. Installation of unauthorised software is restricted through application control.

8. Backup and Recovery

8.1 Backup Strategy

Customer data and service configuration are backed up on a defined schedule, with backups encrypted using AES-256, stored in a separate region from the source, and access-controlled independently from production. Backup integrity is verified, and restore tests are performed on a documented cadence — not merely the existence of backups but their usable recovery.

8.2 Retention and Data Handling

Backups are retained for periods aligned with customer contractual commitments and regulatory expectations applicable to insurance data. Backups containing personal data are included in retention and erasure obligations under the Data Processing Agreement.

8.3 Recovery Objectives

Recovery Time Objectives and Recovery Point Objectives are defined per service and per customer tier, and documented in customer contracts. They are validated through recovery testing rather than asserted.

9. Business Continuity and Resilience

9.1 Continuity Framework

Our Business Continuity Management framework is designed to protect our customers' ability to operate when disruption affects us. The framework covers:

- Business Impact Analysis identifying time-critical processes, their dependencies, and acceptable disruption thresholds.
- Business Continuity Plans for each material operational function.
- IT Service Continuity arrangements focused on the recovery of customer-facing services.
- Crisis Management arrangements for the coordination of response in serious events.
- Exercising programme — continuity plans are tested on a regular cadence, including scenario exercises and technical recovery tests.

9.2 Resilience Architecture

Customer-facing services are designed for regional resilience within Azure, with active-passive or active-active configurations depending on service tier. Dependencies on specific Azure services are reviewed for substitutability where operationally feasible and proportionate.

9.3 DORA and Operational Resilience

The Digital Operational Resilience Act (Regulation (EU) 2022/2554) applies to our in-scope financial-entity customers. We support their obligations through the contractual provisions required under Article 30, through our own continuity testing, and through participation in customer-led concentration-risk and exit-readiness reviews.

10. Incident Response

10.1 Detection

We detect incidents through a combination of automated monitoring, scheduled review, customer reports, and external notifications (including from Microsoft, threat-intelligence partners, and coordinated-disclosure researchers). All sources feed into a single triage process.

10.2 Classification and Response

Incidents are classified by severity and type. A documented response procedure sets out roles, communication paths, escalation thresholds, containment and eradication steps, and evidence-preservation requirements. We maintain a 24-hour capability to engage on critical incidents.

10.3 Customer Notification

Where an incident affects a customer or a customer's data, we notify the customer in line with our contractual commitments — typically as soon as reasonably practicable, and in any event within the timeframes set out in the Data Processing Agreement. Notifications include the information the customer needs to meet its own obligations, including (where applicable) its obligations under Article 33 UK/EU GDPR.

10.4 Regulator Notification

Where we are the controller and a personal data breach meets the threshold in Article 33 UK/EU GDPR, we notify the relevant supervisory authority within 72 hours of becoming aware. Where we are a processor, we assist customer controllers in meeting their notification obligations.

> **DORA Major ICT-Related Incidents**
> For customers in scope of DORA, we support the classification, reporting, and information-sharing obligations that apply to major ICT-related incidents,

> operational-or-security-payment-related incidents, and significant cyber threats. Contractual arrangements define how information is shared to enable customer reporting within the DORA timelines.

10.5 Lessons Learned

Every material incident is followed by a documented post-incident review — root cause, contributing factors, response assessment, and specific actions to prevent recurrence. Actions are tracked through to closure and reported to the Information Security Steering Group.

11. Third-Party and Sub-Processor Management

11.1 Governance

We recognise that our customers' security posture depends in part on ours, and ours depends in part on our suppliers. We therefore operate structured third-party risk management, with suppliers tiered by the sensitivity and criticality of what they do for us.

11.2 Due Diligence

Before engaging a supplier, we assess their security, privacy, financial, and resilience posture proportionate to their tier. For suppliers handling personal data or supporting critical functions we require independent assurance (such as ISO/IEC 27001 certification or SOC 2 Type II reports), documented data-protection commitments, and clear contractual security terms.

11.3 Ongoing Oversight

Suppliers are subject to ongoing monitoring, including periodic reviews, advisory tracking, and where appropriate, audit. Material changes to a supplier's security, ownership, sub-contracting, or geography trigger review.

11.4 Sub-Processors

Where we engage sub-processors to process personal data on behalf of customer controllers, we do so under contracts imposing equivalent obligations, and only with the authorisation required under the applicable Data Processing Agreement. Our current sub-processor list is maintained on our website. Customers are notified in advance of material changes in line with their contract.

11.5 Microsoft Azure

Microsoft Azure is our most significant supplier. We rely on Microsoft's certifications (including ISO/IEC 27001, ISO/IEC 27018, SOC 2, and sector-specific attestations), supplemented by our own configuration, monitoring, and operational controls under the

shared-responsibility model. We maintain a Shared Responsibility Matrix identifying which party is responsible for each control area by service.

12. People and Training

12.1 Joiners

All staff and contractors are subject to screening appropriate to their role and jurisdiction before being given access to systems or data. Contracts include confidentiality and security obligations. Access is granted on a role-based model, not through ad hoc requests.

12.2 Training

All staff complete mandatory information-security and data-protection training within 30 days of joining, and annually thereafter. Role-specific training is provided for engineers, support personnel, and others whose roles carry specific risk — including secure coding, phishing awareness, privileged access, and handling of special category data.

12.3 Leavers

Leaver processes revoke access promptly — in standard cases, by the end of the last working day; in unplanned or risk-based cases, before the individual is notified. Equipment is returned, credentials are invalidated, and customer data is verified as not persisting on personal devices.

13. Customer Responsibilities

Good security is a shared commitment. The cXc platform provides capabilities that are only fully effective if customers also do their part. We recommend and, in some cases, require the following of customers:

- Use the identity and access controls we provide — single sign-on where available, multi-factor authentication, and conditional access aligned with the sensitivity of the data processed.
- Manage user lifecycles promptly — provision, re-provision, and de-provision users as roles change.
- Apply role-based access at the tenant level, consistent with least privilege.
- Communicate the cXc Acceptable Use Policy to users, and enforce it internally.
- Notify us promptly of suspected misuse, compromised credentials, or policy breaches affecting the customer's tenant.
- Engage with our customer-facing change, release, and advisory communications.

14. Contact

Specific contact points for security and privacy matters:

Organisation	cXc — conXchange Pvt Ltd
Security matters, vulnerability reports	info@mycxc.services
Privacy and data protection	info@mycxc.services
Abuse and misuse of the Services	info@mycxc.services
Support	info@mycxc.services
General enquiries	info@cxc.services
Website	https://www.mycxc.services
Postal address	786 London Road, Thornton Heath, Surrey, United Kingdom, CR7 6JB

15. Related Documents

This document is accompanied by a set of formal policies, agreements, and notices which together form our published trust and security framework:

- Privacy Notice — how we process personal data.
- Acceptable Use Policy — rules governing use of the Services.
- Vulnerability Disclosure Policy — how to report security issues.
- Cookies Notice — cookies and similar technologies used on our website.
- Data Processing Agreement — contractual processor terms (provided to customers).
- Sub-Processor List — current list of third parties used to process personal data (on our website).
- Master Services Agreement and Service-Specific Terms — contractual framework (provided to customers).

Detailed security documentation — including our Information Security Management System policies, Statement of Applicability, audit reports, penetration testing summaries, and architectural diagrams — is made available to customers and their auditors under confidentiality arrangements. Requests should be directed through your account contact or to security@cxc.services.

16. Changes to This Document

We may update this document from time to time to reflect changes to our business, technology, services, or legal obligations. The current version is always available on our website. Material changes are highlighted and, where appropriate, notified to customers through our usual service channels.