Information and Data Security at Zurich

Version 2.0 (May 2022)

Contents

1. Overview

The Zurich Insurance Group (Zurich) is a leading multi-line insurer that serves its customers in global and local markets. With about 53,000 employees, it provides a wide range of property and casualty, and life insurance products and services in more than 210 countries and territories. Its customers include individuals, small businesses, and mid-sized and large companies, as well as multinational corporations. Given the nature of its business, Zurich frequently collects, stores and uses significant amount of data to carry out its business, which may include confidential information and/or personal data of commercial and retail customers.

Subsequently, Zurich receives a significant number of Requests for Information (RFI) regarding our IT System Management and Development as well as our Data and Information Security policies, processes and standards. These requests take many forms, although they are most often associated with due diligence where we are in or revising business/contractual arrangements with external parties.

Often these requests are accompanied by specific question sets and/or templates to complete which are specific to the individual request. Such responses require a significant amount of time and effort and can be challenging when short timeframes for replies are allowed. In order to address such challenges, this document provides standard and consistent responses to internal and external customer inquiries regarding Zurich's IT systems management and development, data and information security policies, processes and standards. This document intends to cover the most common areas of information security.

This document is owned by the Global Information Security function of Zurich (Isle of Man) and its content is regularly reviewed to ensure accuracy and completeness.

2. Scope

This document provides generic information regarding policies, process, standards and the presence of technical security measures (such as Anti-Virus) regarding data and its protection at Zurich, but it does not provide details regarding the names, versions, or configurations of the technologies used, as this might compromise the security posture of Zurich.

The recipient of this document undertakes to keep this document strictly confidential and not to share it with third parties (if not agreed by Zurich).

3. Audience

This document is intended for internal as well as external audiences and may be distributed externally in response to inquiries from customers, clients, prospective vendors, regulators and auditors **who are bound by confidentiality obligations**.

4. Zurich's Code of Conduct

Zurich's Code of Conduct articulates the key rules of conduct by which we abide to help ensure that we conduct our business activities in accordance with applicable law and high ethical and professional standards.

Zurich's Code of Conduct applies to all employees of Zurich Insurance Group Ltd, its subsidiaries and affiliates worldwide. In addition, we expect third parties who work on Zurich's behalf, such as contractors or agents, to adhere to the spirit of the Code.

Zurich's Code of Conduct clearly highlights that protecting data and safeguarding confidential information is a priority for Zurich. It ensures we take appropriate measures against the unauthorised or unlawful processing of data that Zurich maintains and against its accidental loss, access, destruction or damage.

All Zurich employees are expected to:

- Safeguard confidential information of Zurich, its employees, its customers, business affiliates and other stakeholders through its entire lifecycle, from origin to safe disposal.
- Collect, process and share personal data only for specified, legitimate and required purposes and only to the extent necessary.
- Access, use and disclose confidential information only on a need-to-know basis and when authorised for a legitimate business purpose.

- Respect privacy rights and preferences of the persons whose data we process.
- Ensure that electronic personal data or confidential information is protected in transmission and storage through adequate technical safeguards.
- Report data security breaches through appropriate management channels as quickly as possible.

5. Policies, Standards and Responsibilities

Zurich has a global information security framework incorporating standards owned by its Global Information Security function and approved by the Board of Directors of Zurich Insurance Group Ltd.

Our information security standards and policies are designed to:

- Protect information assets from loss and unauthorised access, modification, and/or destruction.
- Ensure and enforce appropriate handling of data according to use and classification.
- Meet regulatory, compliance and audit requirements.
- Ensure that data is retained only if it is lawfully required.
- Ensure Data Subjects are fully aware of their rights under applicable data protection laws and regulations including the EU GDPR.

Zurich also has dedicated Architecture, IT Governance, and Supplier Assurance functions, each with formal processes, checkpoints and approval processes. These provide robust management, audit and oversight of these related functions.

While the Zurich Insurance Group is responsible to establish and maintain group policies and standards in the foregoing areas, it is the responsibility of its worldwide subsidiaries and affiliates to adopt and implement these policies and standards locally. Where the policy is not met an exception must be sought and approved by senior management.

Our policies are reviewed annually but are not publicly available. They include the following:

Information Security, Data Handling and Classification

- Information Classification
- Storage and Cryptography
- Data Decommissioning
- Physical Security
- Mobile/Portable Devices and Policies

Access Management

- Application and Data Ownership
- Application Security/Configuration
- Password/Access Control Statement
- User Recertification

Systems Development and Change

- Application Development
- Separation of Production from Development and Test Environments
- Data Quality Controls
- Documentation of Developments
- Testing Requirements
- Audit Trail Requirements
- Deployment to Live
- Patch Management Statement

Human Resource Management

- Staff Screening
- Accounting of Assets from Terminated Employees

Business Continuity Statement

- Hardware Requirement and Safeguards
- Backup Statement and Replication
- DR and Business Continuity Plans
- Crisis Management Statement and Major Incident Statement

Privacy Statement

- Privacy Principles
- Privacy Risk Driver Evaluation
- Privacy Awareness and Training
- Privacy Controls and Processes
- Reporting
- Responsibilities

IT Security/Cyber Risk

- Computer Security Event Log Management Standard
- Cryptography
- Enterprise Patch Management
- Media Sanitisation
- Global Identity Access Management Standard
- Global IT Usage
- SAP Global Patch Management
- WiFi Guest Access Security Standard

Other Policies of Interest

- Vendor Assessment Controls
- Information Security Training
- Regular Security Assessments
- Service Management Standards
- Independent Audit Report
- Entitlement Statement/Process
- Physical Access

6. Audit and Review

Controls set forth in the Zurich IT Risk Standards and Consolidated IT Controls Catalogue (CITCC) and Cyber Policies are reviewed at least annually, or more frequently in the event of material change. Standards and Guidance are updated every two years or more frequently in event of material change.

In addition to a comprehensive schedule of internal assessment – both self-certification and by Zurich Group Internal Audit – processes, procedures and locations are in scope for assessment by Zurich's external auditor.

7. Regulation and Certification

Zurich is an insurance company and not a supplier of IT services; therefore, we have not sought to obtain ISO (International Standards Organization) certification. However, we do comply with best practice data information security policies and measures are in place which align with the requirements of the ISO 27001, ISO27K, NIST, CIS and COBIT standards framework, as set out in the Zurich IT Risk Standards and Consolidated IT Controls Catalogue (CITCC). Zurich's third-party suppliers are contractually obliged to provide assurances to Zurich that as IT service providers they apply appropriate data security to our data including, but not limited to, by complying with/attaining certifications with standards such as ISO 27001, ISAE 3402 and AA01/06, in addition to completing a Controls Self-Assessment.

In addition to the above we also monitor both industry and general best practices, such as ISO, NIST, CSF, and ENISA, and keep abreast of requirements (such as Cyber Essentials).

8. Data Commitment

Going beyond legal requirements, Zurich's data commitment includes a promise never to sell customers' personal data nor to share personal data without being fully transparent, meaning customers will always be notified if their personal data is shared, and with whom. Further, any third party with whom Zurich does share personal data is bound by an enforceable contract, which sets out how that personal data can be used. The four promises to customers in Zurich's data pledge are to:

- Keep their data safe
- Never sell their personal data
- Not share their personal data without being transparent about it
- Put their data to work so Zurich can better protect them, and so they can get the most out of life.

https://www.zurich.com/en/sustainability/customers/zurich-data-commitment

9. Zurich Employees

It is Zurich's policy to screen all candidates who are issued an employment contract, whether permanent or temporary, as part of the recruitment process – subject to and to the extent allowed by local law or regulation.

Vetting is inclusive of: e.g., identity checks and reference and CV checks. Additional vetting is applied to Key Function Holders, including e.g., criminal record checks.

Additional vetting/assessment may be required for specific roles or responsibilities.

It is also a requirement for Zurich's third-party strategic suppliers to perform vetting of all their staff who are engaged on the Zurich account. Contractor and vendor agreements for contracts requiring the handling of data require similar screening for staff assigned.

10. Education and Awareness

All Zurich employees are required to undertake a suite of mandatory on-line education and awareness training.

This covers Data/Information Security, Data Protection, Records Retention, Anti-Money Laundering, Trade and Economic Sanctions, Anti-Fraud and Zurich's Code of Conduct and associated knowledge confirmation assessments. This training is required upon joining Zurich, and then at regular intervals thereafter. Further targeted training is provided for specific roles. Zurich also has an ongoing program of security education and awareness for all staff. This is included in the mandatory annual training but is further supported by periodic email phishing simulations and educational opportunities. During the month of October, Zurich promotes security awareness to Zurich employees through a series of education and awareness events.

It is also a requirement for service providers and vendors to be trained and operate in compliance with our data privacy and security standards as they relate to the services provided. Procedures are in place to ensure that physical and information access to assets is withdrawn when an employee leaves the company.

11. Requirements and Disciplinary Action

Data Security requirements are reflected in Zurich policies, and employees are expected to comply with all policies as a condition of employment. Violations of any company policy are subject to Zurich's standard HR processes and may result in disciplinary action – up to and including dismissal.

12. Incident Management

We consider a data security incident to be an event impacting the confidentiality, integrity or availability of data (there are varying levels of severity).

Zurich uses a formal incident reporting, management and resolution process with a defined set of response levels and escalation paths, depending on the severity of the event.

All systems run under an agreed operational response framework which is reviewed periodically within our dedicated service management organisation. This covers security/system incidents and disaster recovery (DR) scenarios.

Dependent on the severity of the incident or DR situation, the organisation has three levels of response teams (gold, silver and bronze) that will be invoked accordingly. The teams are responsible for the co-ordination and management of the incident until resolution. Zurich maintains a 24x7 support for security incidents in all our regions.

13. Data Classification and Ownership

All information assets are the responsibility of defined Information Owners within the organisation. Information Owners maintain an inventory of information assets within their ownership.

13.1 Classification

Zurich information must be classified in accordance with Zurich's classification schema. There are four defined classification categories:

- **Public**
- **Internal use only**
- **Confidential**
  - Personal Data
  - Non-Personal Data
- **Highly Confidential**
  - Personal Data
  - Non-Personal Data
  - Sensitive Personal Data

Mandatory requirements for data handling (including storage, sharing, encryption, retention and destruction) are defined for each classification. This is documented in the Zurich Risk Policy (Information Risk Policy Manual (MR 5G), Section 3.1 – Data Classification).

13.2 Personal Data and GDPR Compliance

Zurich International Life Limited is a wholly owned subsidiary of Zurich Insurance Group Switzerland. We provide financial services from the Isle of Man and our branch network. We are regulated by the Isle of Man Financial Services Authority. We are licensed and/or authorised in the respective regions in which we operate. We comply with Isle of Man Data Protection law which includes the EU GDPR; and the regional data protection laws and regulations in the countries where we operate. Zurich is a Data Controller registered with the Isle of Man Information Commissioner https://www.inforights.im/

Personal data is any information related to an identified or identifiable individual. It is Zurich policy to classify personal data as confidential and sensitive personal data as highly confidential and to protect it accordingly.

At Zurich we take our data protection obligations very seriously. Zurich greatly values the trust our customers, claimants, employees and others place in Zurich when they share their data and, because of this, the security of that data is of paramount importance to Zurich. Zurich relies on personal data of customers to accurately and effectively assess risk, provide customers with coverage that meets their needs, and to settle claims. While all the data we use are important, Zurich treats data about individuals – such as our personal lines customers and employees – with the greatest care and respect. Zurich has given a public commitment to data privacy details of which can be found here https://www.zurich.com/en/sustainability/customers/zurich-data-commitment

13.3 Retention and Destruction

Zurich is committed to ensuring that records are appropriately and adequately protected, maintained and discarded at the proper time. We have formal record retention schedules for all areas, setting out the document retention rules, which vary depending upon the nature of the data.

Typically, records are maintained for a minimum of 6 years after the termination of a customer relationship but in some circumstances, records will have a longer retention period based upon regulation in the jurisdiction.

Data is disposed of in a secure manner when no longer required (including any Legal Hold and/or retention requirements) by using methods that meet regulatory requirements and best practice, for example:

- Electronic records are deleted by overwriting to recognised industry standards, degaussing drives or physical destruction of media.
- Confidential paper media is held in secure waste bins, shredded and/or incinerated.

13.4 Transmission, Storage and Encryption

Any communication of data outside the Zurich network is encrypted in line with policy requirements.

Within the Zurich network security techniques are employed for storage, including encryption, and are based on context and data in scope. This will also apply to data stored/processed by Zurich third parties/suppliers.

13.4.1 Cryptography

Zurich has defined standards regarding cryptography and encryption. Specific details relating to deployment and configuration are confidential and we would therefore generally not share this information, however, below is an example of minimum recommended standards:

- Symmetric Primitive: AES – key length of at least 128 bit (256 preferred)
- Cryptographic Hash: SHA-2, SHA-3 – key length of at least 256 bit
- TLS/SSL Protocol: TLS 1.2 or later (using DHE or ECDHE for key exchange)

14. Data Centres and use of Cloud Services

Zurich International Life operates from primary and recovery data centres using our own dedicated infrastructure. Our two main data centres are located on the Isle of Man (one main centre and one for disaster recovery). Both are hosted by Manx Telecom with real time replication between them. All our data centres are ISO accredited (ISO-27001, ISO-14001 & ISO-9001) and as a minimum, meet the Tier 3 data centre standard.

https://www.manxtelecom.com/about/certifications

In addition, we use the Zurich Group public and private cloud services, which include AWS (Amazon Web Services) and MS (Microsoft) Azure, for data and some application hosting that support several business processes.

We and our Group conduct rigorous due diligence on all suppliers, and they are required to meet our strict security standards for the hosting of data including, but not limited to, access control and encryption of data in transit and at rest. Cloud suppliers may be subject to additional assessment via our cloud governance process.

15. Disaster Recovery (DR)/Business Continuity Plan (BCP)

We maintain a comprehensive set of business continuity plans that cover all critical aspects of our operations including people, process and system accessibility. Zurich is dedicated to regular testing and exercising of its business continuity capability to ensure we remain resilient.

The Zurich workforce can work remotely from any secure location using Virtual Desktop Technology and/or secure VPN. As such, if any Zurich office is closed for any reason, normal business operations will continue without interruption.

IT disaster recovery exercises of critical applications are conducted on an annual basis. This is to prove that the RTO (recovery time objective)/RPO (recovery point objective) requirements can be achieved in the event of a true disaster at one of our primary data centres. Disaster recovery capacity allows for full recovery of the production environment that includes all production applications from an affected primary data centre.

15.1 Incident Response Programme

We maintain a comprehensive data security incident response plan to effectively and securely address potential data security incidents. The incident response programme includes an incident response team, documented procedures for the identification and investigation of an Incident, notification of stakeholders, containment, analysis, tracking, repair, recovery and remediation.

Zurich Group's Cyber Incident Response Team (CIRT) provide global coordination of multiregion incidents across the wider Group. It coordinates with several of Zurich's internal groups as appropriate to ensure an effective response to all large scale computer security Incidents.

16. Access Control

Zurich's Identity and Access Management policy ensures access is granted in line with role and responsibility based on least privilege[1]. Access is managed centrally via our Identity and Access Management System.

Users have unique IDs and passwords, which must never be shared. Both preventative and detective processes and technical controls are in place to enforce separation of duties. Access rights are subject to regular recertification.

Well-defined processes for joiners, movers and leavers ensure this policy is maintained.

16.1.1 Privileged Accounts/Admin Access

Admin access requires system approval and, depending on the access, may be subject to regular recertification.

We also utilise credential vaulting and enhanced logging for admin accounts.

17. Authentication Mechanisms Standard

Zurich has an Acceptable Authentication Mechanisms standard in place, which specifies the use of acceptable authentication mechanisms within Zurich, which at a minimum, allows the use of one or more authentication token factors (something you know, have, and are) using a secure authentication protocol, either:

1. Single Factor: A token that uses one of the three factors (know, have and are) to achieve authentication.
2. Multi Factor: A token that uses two or more factors (know, have and are) to achieve authentication.

Allowed token types for authentication:
Memorized Secret Tokens (passwords, passphrases etc.), Pre-Registered Knowledge Tokens, Look-up Secret Tokens, Out of Band Tokens, and Single Factor One-Time Password devices, Single-Factor Cryptographic Device, Multi-Factor Software Cryptographic Token, Multi-Factor One-Time Password Device, Multi-Factor Cryptographic Devices are allowed.

The Acceptable Authentication Mechanisms standard applies to Zurich data, systems, applications, activities and assets owned, leased, controlled or used by Zurich, its agents, contractors or other business partners on behalf of Zurich.

[1] 'Least privilege' is an access principle according to which users must be provided the minimum system/application functionality required to perform their job.

18. Network and Device Security

Zurich has a layered approach to security that, for externally facing systems, incorporates, but is not limited to: Firewalls, IPS, DDoS protection, Data Leakage Prevention (DLP), load balancing, etc. We also perform regular perimeter and network vulnerability scanning and penetration testing. At network level this includes elements such as anti-virus, IDS, APT detection as well as device hardening to ensure access to components such as routers and switches is restricted to authorised users only on a “least privileged” basis.

Network architecture is documented (critical networking components, connections and data flows), reviewed and updated on a regular basis.

Prioritisation of application/system protection is focused on classification of data held in or processed by the system/application and business criticality.

Security of workstations and mobile devices is centrally managed and implements controls around the use of portable media. Controls such as AV, DAC, DLP and device encryption apply at this level.

18.1. Email Security and Privacy

It is our statement and practice to only use secure methods of file transfer and exchange. For example, to maintain the security and privacy of email communications, we support both enforced and opportunistic TLS/SSL, and PGP encryption. Mail servers support opportunistic TLS/SSL 1.2, automatically encrypting messages to servers that are similarly configured.

19. Zurich International online (ZIO)

If you are purchasing corporate savings services from us, you will be offered access to ZIO, our web portal. ZIO delivers reporting information to individual members and/or Groups and has some transaction capability. The external interface is load balanced with DDos protection enabled. It is protected from cyber-attacks such as those identified in the MITRE attack framework including threats like cross-site scripting (XSS), SQL injection (SQLI), cross-site request forgery (CSRF) and remote file inclusion (RFI), DDoS and others, using Next gen Cloud WAF technology.

ZIO uses a security cookie containing a ZIO user authentication token, which persists for 15 seconds. It can also be integrated into single sign-on environments using Security Assertion Mark-up Language (SAML) 2.0.

20. Mobile Devices

Enterprise Mobile Device Management, Mobile Application Management solutions and Conditional Access Policies for cloud access are in place to enable secure use of approved mobile devices.

21. Removable Media

Use of removable media (USB and Optical ports/drives, etc.) is disabled by default via centrally managed endpoint controls or restricted such that transfer of data can only be made to an encrypted drive. Usage is by exception only. Only approved media/devices may be used, and encryption is enforced.

22. Internet Access

Internet access is via a Zurich centrally managed gateway. Security settings are enforced on all devices.

23. Remote Access

Remote access is permitted for approved users only and is strictly via corporate SSL VPN, utilising two-factor authentication, a comparable method of advanced authentication, or secure Citrix connections.

24. Wi-Fi

Wi-Fi connections to the corporate network require two-factor authentication and/or registration and are subject to WPA2 security.

Guest Wi-Fi access is segregated from the corporate network; this also requires authentication (via Zurich provisioned and controlled account) and is subject to WPA2 security.

25. System Hardening

Zurich maintains technology product specific mandatory security hardening standards which contain instructions or procedures for configuring a product prior to entering the Zurich production environment. In conjunction with regular configuration scanning this ensures a consistent minimum-security baseline is maintained throughout the organisation.

26. Patching

Zurich has a consistent approach to server and application vulnerability management and patching. Scanning is frequent and supports the patching cycle which is monthly for standard (e.g. version upgrade) patches and expedited as appropriate for critical (e.g. security) patches. The details of this process are confidential.

27. Monitoring and Logging

Regular scanning/auditing of both network perimeter and internal components and applications is conducted by Zurich's Global Information Security function.

Logging varies by application/system but typically includes as a minimum user activity (log on, log off, failed authentication attempts, etc.). These are monitored by a Security Technology Operations team within Zurich's Global Information Security function.

28. System and Software Development Life Cycle (SDLC) Management

Material system changes and developments adhere to a formal, mature system development methodology.

Project Z is Zurich's project management framework. This framework sets Key Milestones that are as a minimum required to ensure successful project delivery. Project Z strongly focuses on program/project Key Milestones to be achieved throughout the lifecycle of the project with clear outcome of each milestone.

Changes are developed in a non-production environment and escalated to production environments following appropriate testing and change control processes.

Changes to the final environments (production and user acceptance test) are made by independent and dedicated non-project development teams, maintaining segregation of duties.

29. Change Management

Zurich has an operational change management process where standardised methods and procedures are used for efficient and prompt handling of technical changes, in order to avoid change-related incidents and minimise their impact upon service quality, and consequently to improve the day-to-day operations of the organisation.

Changes (normal, standard, emergency and expedited for major projects or small fix) are governed and audited by a change approval board (CAB – Change Advisory Board), with formal implementation and change approval needed by these before they can be implemented.

30. Use of Data for Testing

Each level of our development lifecycle uses its own specific test data. No live production, commercially sensitive or personal data is used or accessible outside the production system without the implementation of appropriate compensating controls. Where such data may be needed to replicate certain situations a formal exceptions process is in place and any data first undergoes a rigorous masking process where appropriate before being passed to any non-production authorised personnel.

31. Application Security Testing

Applications are tested for security vulnerabilities throughout the Software Development Life Cycle (SDLC). The Zurich security assurance seven stage SDLC process consists of Planning, Analysis, Design, Development, Testing and Integration, Deployment and Maintenance. Application security testing performed during the SDLC includes: code reviews, static and dynamic testing, interactive testing and penetration testing. Vulnerabilities discovered are prioritised, tracked and remediated to ensure Zurich data is always secure.

32. Physical Security

Access to buildings is typically controlled via proximity card-based access control systems and is through staffed reception areas for larger locations. The issue of passes to Zurich employees, contractors and guests to access the buildings is authorised by local Corporate Real Estate & Workplace Services (CRE&WS) or other local responsible function (e.g., Corporate Investigations and Security Services), as applicable.

Access to server rooms and rooms containing network equipment is further restricted as necessary (e.g. only IT staff have the ability to enter server rooms). Depending on location and purpose of visit, visiting external engineers may be required to sign in at reception and be escorted at all times whilst on site by a Zurich employee.

33. Visitors

Visitors are required to sign in at reception and be escorted at all times whilst on site by a Zurich employee. All visitors must comply with Zurich security policies.

34. Asset Inventory

An inventory of physical IT assets is maintained by Group Operations & Technology.

35. Third Parties

All third parties (vendors, suppliers, etc.) provide services under contract and Zurich has a robust and comprehensive supplier assurance and governance framework to ensure third parties and business partners meet our minimum standards in all areas – including security and data protection.

Important information

Zurich Integrated Benefits is a business name of Zurich International Life Limited.

Zurich International Life Limited is authorised under the Isle of Man Insurance Act 2008 and is regulated by the Isle of Man Financial Services Authority which ensures that the company has sound and professional management and provision has been made to protect planholders.

For life assurance companies authorised in the Isle of Man, the Isle of Man's Life Assurance (Compensation of Policyholders) Regulations 1991 (as amended), ensure that in the event of a life assurance company being unable to meet its liabilities to its planholders, up to 90% of the liability to the protected planholders will be met.

The protection only applies to the solvency of Zurich International Life Limited and does not extend to protecting the value of the assets held within any unit-linked funds linked to your plan.

Zurich International Life Limited is not authorised to offer insurance products for sale in the United States.

Materials are not intended as an offer to invest and do not constitute an offer or a solicitation of an offer to buy securities in any other country or other jurisdiction in which it is unlawful to make such an offer or solicitation.

Zurich International Life Limited (a company incorporated in the Isle of Man with limited liability) provides life assurance, investment and protection products and is authorised by the Isle of Man Financial Services Authority.

Registered in the Isle of Man number 20126C.
Registered office: Zurich House, Isle of Man Business Park, Douglas, Isle of Man, IM2 2QZ, British Isles.
Telephone +44 1624 662266   Telefax +44 1624 662038   www.zurichinternational.com

ZURICH®