Information and Data Security at Zurich

Version 3.0 (November 2024)

Contents

1. Overview and Contractual Context

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

This document outlines Zurich's policies, processes, standards, and the technical security measures in place to protect data, including those implemented by Zurich International Life Limited and its branches.

Our products and Records

As a regulated insurance company, Zurich provides insurance, employee benefits, and insurance based personal savings contracts to our valued customers. We are legally required to maintain records of our activities under applicable laws, regulations, and any contracts (direct or indirect) with data subjects. The information we hold is obtained in our capacity as a regulated insurance company and data controller, representing our company's records.

For clarification, Zurich does not provide IT services, hosting services, data processing activities, or maintain your company's records under the insurance contracts between us. However, in our role as the data controller over our records and at our discretion; we may allow scheme members or company pension scheme administrators to view records related to them via our web portal: Zurich International online (ZIO) and ZIO Members App.

Privacy and external certifications

While we strive to provide our customers with confidence and assurance regarding the privacy of our systems and to fulfil reasonable information requests, we, like most financial institutions, do not comment on or disclose details about confidential matters that could compromise our security posture.

Numerous IT security frameworks and standards operate globally. Individual standards recognised in some geographical regions but not others. This creates a challenge for a globally regulated business. Companies such as Zurich must operate under a unified security framework which forms the foundation of any security strategy. Since no single standard framework fully meets the global requirements we must achieve, Zurich has developed its own global framework and has based it upon on the requirements of the most globally recognised standards, ISO 27001, ISO 27K, NIST, CIS, and COBIT frameworks. We apply our framework across all our operations.

Zurich's third-party suppliers are contractually obligated to ensure the security of our data by implementing appropriate data security measures. These measures include, but are not limited to, complying with or attaining certifications for standards such as ISO 27001, ISAE 3402, and AA01/06, as well as completing a Controls Self-Assessment.

In common with most regulated financial institutions that provide financial services rather than IT services, we have not pursued external certification of our framework.

2. About us and Privacy

Zurich Insurance Group Ltd ("Zurich") is a leading multi-line insurer serving people and businesses in more than 200 countries and territories and has about 60,000 employees. Founded more than 150 years ago, Zurich is transforming insurance. In addition to providing insurance protection, Zurich is increasingly offering prevention services such as those that promote wellbeing and enhance climate resilience. Reflecting its purpose to 'create a brighter future together,' Zurich aspires to be one of the most responsible and impactful businesses in the world.

Zurich is committed to the highest standard of data privacy. We only use personal data for legitimate and specified purposes and only keeps it for as long as needed. We communicate transparently about how we use your data and the measures we have in place to protect it. We have issued a commitment to Data Privacy and Protection to provide assurances about how we handle the information we receive in connection with the insurance business we conduct.

Zurich International Life Limited (ZILL) is part of Zurich. Headquartered on the Isle of Man, we offer life insurance, investment, and protection solutions to support our customers in more than 215 countries and territories from our operations in the Isle of Man, United Arab Emirates, Bahrain, Qatar and Hong Kong. We work with the Zurich Global Cyber Information Security function to protect our information assets.

The Isle of Man is a self-Governing Crown Dependency situated between England and Ireland. During August 2018, the Isle of Man Parliament incorporate EU GDPR into its legislation. The European Commission has recognised Isle of Man legislation as "Adequate", meaning "personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.

In January 2024 The EU published its findings on IOM GDPR which are contained in pages 155-181 of their report entitled: Country Reports on the functioning of the adequacy decisions adopted under Directive.

3. Policies and Standards

Our information security standards and policies, although not publicly available, are reviewed annually and approved by the Board of Directors of Zurich Insurance Group Ltd., They are designed to: -

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

Zurich also maintains dedicated Architecture, IT Governance, and Supplier Assurance functions, each supported by formal processes, checkpoints, and approval procedures. These functions ensure robust management, audit, and oversight, reinforcing our commitment to excellence and security across these critical areas.

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

4. Security Control Framework

Zurich ensures IT system security through our dedicated global Zurich Group Security teams, comprising approximately 620 IT and cyber security specialists. These teams operate around the clock, providing 24/7 coverage, 365 days a year, across different regions. They are tasked with monitoring and protecting our systems, driving, and enforcing a mandatory framework of policies, processes, and controls throughout Zurich's infrastructure.

The absence of a unified international data security standard prompted Zurich to develop its own comprehensive corporate controls framework, incorporating cross-regional standards. Our framework draws upon established standards, including NIST CSF, NIST 800, ISO 27001/2, CIS Top 20, and COBIT. This framework is overseen by our global Zurich Information Security function and has been approved by the Board of Directors of Zurich Insurance Group Ltd.

4.1 Controls

The standards are documented in the Zurich Consolidated Controls Catalogue which covers the following control headings and is updated every 2 years or more frequently in event of material change: -

Access Control

- AC1 - Principles of Least Privilege
- AC2 - Identification, Authentication and Privileged Access.
- AC3 - Access Management Lifecycle and Recertification
- AC4 - Documentation
- AC5 - External Access
- AC6 - Physical Access

Service Management

- SM1 - Security Architecture
- SM2 - System Documentation
- SM3 - Asset Management
- SM6 - SLA Approval
- SM7 - Secure Network Access
- SM8 - Malware Protection
- SM9 - Intrusion detection and Vulnerability Management
- SM11 - Network Devices
- SM12 - System Configuration
- SM13 - E-Mail & Messaging
- SM14 - Incident response

Compliance and retention

- CR1 - Roles & responsibilities
- CR2 - Business Requirements
- CR3 - Information Security Training
- CR4 - IT Risk Assessment
- CR5 - Security Assessment
- CR6 - Loging & Monitoring

Systems Development and Change

- SD1 - Methodology
- SD3 - Security by Design Principal
- SD4 - Web Applications
- SD5 - System Standards
- SD6 - Change Management

Data Security

- DS2 - Protection of Data
- DS3 - Cryptographic Controls

Resilience

- DR1 - Critical System Resilience
- DR2 - Systems Backup
- DR3 - Disaster Recovery

4.2 Compliance - Attestation, Review and Audit

Adherence to security measures is ensured through quarterly control attestations by each business unit (BU), which cover control design and operational effectiveness. This process is complemented by regular reviews conducted by an independent team, along with internal audits, to maintain the highest standards of security and integrity and external financial audits for statutory accounts.

5. Physical Security

Access to buildings is controlled via proximity card-based access control systems, electronic gates and is through staffed reception area. The issue of passes to Zurich employees, contractors and guests to access the buildings is authorised by Zurich Corporate Real Estate and Workplace Services (CRE&WS).

Windows are sealed and CCTV operates throughout the building and in sensitive areas. Access to sensitive areas including switch and server rooms containing network equipment is further restricted to authorised IT staff by electronic door pin and card.

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.

6. Access Control

Zurich's Identity and Access Management policy ensures access is granted in line with role and responsibility based on least privilege . Access is managed centrally via our Identity and Access Management System. Well-defined processes for joiners, movers and leavers ensure this policy is maintained.

6.1 User Accounts

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

6.2 Privileged Accounts / Admin Access

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

6.3 Remote Access

Remote access is permitted for approved users only and is strictly via corporate SSL VPN, utilising 2-factor authentication, a comparable method of advanced authentication, or secure Citrix connections.

6.4 Internet Access

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

6.5 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.

7. Authentication Mechanisms Standard

We adhere to an Acceptable Authentication Mechanisms standard established by Zurich Group. The standards ensure the use of appropriate authentication methods within our organisation. These standards mandate the use of one or more authentication token factors (something you know, something you have, and something you are) combined with a secure authentication protocol.

The Acceptable Authentication Mechanisms standard is applicable to all Zurich data, systems, applications, activities, and assets that are owned, leased, controlled, or used by Zurich, including those managed by our agents, contractors, or other business partners on behalf of Zurich.

8. Asset Inventory

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

9. Data Centres

Zurich International Life Limited maintains twin Data Centres on the Isle of Man for its systems of record. Both Data Centres are built to Tier 3 standards. A Tier 3 Data Centre has multiple paths for power and cooling and systems in place to update and maintain it without taking it offline. It has an expected uptime of 99.982% (1.6 hours of downtime annually).

The data centres are owned and operated by Manx Telecom who are responsible for the buildings, connectivity, power and physical security. The data centres are ISO accredited (ISO-27001, ISO-14001 and ISO-9001) https://www.manxtelecom.com/about/certifications.

The dedicated infrastructure and software in each data centre is owned by Zurich. It is operated and configured by Zurich International Life Limited staff. We have deployed real time replication between our infrastructure in each site (Primary data centre and Recovery data centre) to ensure continuous protection against unexpected outages. Importantly, Manx Telecom have no access to the data.

Both data centres are protected by Zurich Group configured protections which comprised of multi layered protections including anti-virus, anti-malware, intruder protections, next generation firewalls, web application firewalls, access management, vulnerability scanning, patching as described below.

10. Network and Security

At Zurich, we uphold a robust and multi-layered security strategy for our externally facing systems. This strategy encompasses, but is not limited to, next generation firewalls and WAF, Intrusion Prevention Systems (IPS), Distributed Denial of Service (DDoS) protection, Data Leakage Prevention (DLP), and load balancing.

10.1 Documentation

We maintain documentation of our network architecture, covering critical networking components, connections, and data flows. This documentation is subject to regular review and updates to ensure its accuracy and relevance.

10.2 Security Measures

On the network level, our security measures include anti-virus protection, Intrusion Detection Systems (IDS), Advanced Persistent Threat (APT) detection, and device hardening. This ensures that access to critical components such as routers and switches is restricted exclusively to authorised users, adhering to the principle of "least privilege." The prioritisation of application and system protection is determined by the classification of data they handle and their business criticality.

10.3 Network segmentation

We implement network segmentation zones to secure the access to information on a need-to-know basis

10.4 Workstations and Mobile Devices

Our approach to securing workstations and mobile devices is centrally managed, implementing stringent controls around the use of portable media. At this level, controls such as anti-virus (AV), Data Access Control (DAC), Data Leakage Prevention (DLP), and device encryption are rigorously applied.

10.5 Wi-Fi

Our corporate network cannot be accessed by Wi-Fi. While there is a guest Wi-Fi network using WPA2 security it is segregated from and cannot connect to the corporate network.

10.6 Assurance

Regular perimeter and network vulnerability scanning, across the whole Zurich network is combined with local comprehensive penetration testing by qualified third parties helps to protect our information assets and demonstrates our commitment to security.

11. System Configuration/Management

11.1 Hardware and Software

We have implemented baseline configuration incorporating security principles, segregation of duties both intra office and across the organisation for hardware and software. We utilise credential vaulting and enhanced logging for admin accounts. Local users are prohibited from having local administrative rights on workstations and laptops.

11.2 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.

11.3 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.

11.4 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.

11.5 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)

12. 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.

13. Supplier Management

We have a comprehensive supplier management, assurance and governance framework to ensure third parties and business partners meet our minimum standards. All third parties (vendors, suppliers, etc.) provide services under contract. Framework coverage includes but is not limited to background checks, sanction screening, financial viability, IT security, cyber security, AI, use of sub-contractors, environmental governance, human rights and modern slavery.

14. Cloud Services

Where we use cloud services, the provider must meet stringent IT and Cyber requirements of the Zurich Group. Before engaging a service a dedicated all-encompassing review is conducted by ourselves with the support of the Zurich Group's Central Security team's and their third-party security specialist Cyber GRX.

As a Group, Zurich has purchased a number of dedicated Microsoft Azure private cloud service 'Tenants' split by region. The Tenants are used for email, video conferencing via MS Teams, and interoffice collaboration functionality using Office 365. ZILL utilises the European Tenant located in Ireland and the Netherlands meaning that the resulting data is located in Europe.

Our email service supports 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.

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. Incident Management

At Zurich, we prioritise maintaining a comprehensive data security incident response plan to efficiently and securely handle potential data security incidents. Our programme includes a dedicated incident response team and well-documented procedures for identifying, investigating, notifying stakeholders, containing, analysing, tracking, repairing, recovering, and remediating incidents.

We classify a data security incident as any event that affects the confidentiality, integrity, or availability of data, acknowledging that incidents can differ in severity.

Zurich has established a formal process for incident reporting, management, and resolution, with defined response levels and escalation paths based on the severity of the event. Depending on the severity of the incident or DR situation, Zurich activates one of three tiers of response teams—Gold, Silver, and Bronze. These teams are responsible for managing and coordinating the incident until it is fully resolved. Zurich provides 24x7 support for security incidents across all our regions.

If required, the Zurich Group's Cyber Incident Response Team (CIRT) is responsible for global coordination of multi-region incidents across the Group. CIRT works closely with various internal teams within Zurich to ensure an effective response to significant computer security incidents.

16. 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 Wi-Fi 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.

17. 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.

18. System and Software Development Lifecyle (SDLC) Management

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

Zurich's project management framework sets Key Milestones that are as a minimum required to ensure successful project delivery. The framework 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.

18.1 Application Security Management

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.

18.2 Hardware Replacement Programme

We maintain a hardware replacement programme which operates on a 5-year cycle. Prior to any physical media decommissioning, it is processed using military standard secure data removal techniques before physical destruction. This policy extends to disks in any form and memory.

18.3 Software versions policy

We comply with the Zurich Group policy to maintain software versions between N-1 to N-2 depending upon software function, criticality and system.

18.4 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.

19. 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.

19.1 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.

19.2 Personal Data and GDPR Compliance

Zurich International Life Limited is a wholly owned subsidiary of Zurich Insurance Group Ltd. 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's 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/sustainability/data-privacy-and-protection

19.3 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.

19.4 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 7 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.

20. Personnel

As a regulated Insurance company Zurich has established processes around employee management to meet the regulations in the locations where we operate.

20.1 Personnel Screening

Zurich screens all employees, whether permanent or temporary, as part of the recruitment process. The screening includes identity, reference and CV checks – subject to the extent allowed by local law or regulation. Additional vetting is applied to Key Function Holders, including e.g., criminal record checks.

We also require our 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.

20.2 Education and Awareness Training

Zurich also has an ongoing program of security education and awareness and testing for all staff. All employees are required to undertake annual mandatory on-line education and awareness training. The topics include 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. Further targeted training is provided for specific roles. All employees are involved with periodic email phishing simulations.

We require 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.

20.3 Zurich's Code of Conduct

Zurich has established a Code of Conduct that defines the essential principles that guide us in conducting our business with integrity, in compliance with the law, and upholding the highest ethical and professional standards. The Code applies universally to all employees of Zurich Insurance Group Ltd, including its subsidiaries and affiliates globally. We expect contractors, agents, and other third parties acting on Zurich's behalf to embrace the spirit of our Code.

A cornerstone of Zurich's Code of Conduct is the protection of data and the safeguarding of confidential information. We are committed to taking all necessary measures to prevent unauthorised or unlawful processing of the data we handle, as well as its accidental loss, access, destruction, or damage.

Zurich employees are entrusted with the following responsibilities:

Protect confidential information: Safeguard the confidentiality of Zurich's information, including that of our employees, customers, business partners, and stakeholders, throughout its lifecycle—from creation to secure disposal.

Responsible data handling: Collect, process, and share personal data only for specific, legitimate, and necessary purposes.

Need-to-know basis: Access, use, and disclose confidential information only when authorised and for legitimate business purposes.

Respect privacy: Honor the privacy rights and preferences of individuals whose data we process.

Technical safeguards: Ensure electronic personal data and confidential information are protected during transmission and storage with appropriate technical measures.

Prompt reporting: Report any data security breaches immediately through the proper management channels.

Data security requirements are embedded in Zurich's policies, and employees are required to adhere to these policies as a condition of their employment. Any breach of company policy will be addressed through Zurich's standard HR procedures and may lead to disciplinary actions, including potential dismissal.

21. Client Web Portal - Zurich International Online ("ZIO")

If you are purchasing a corporate savings service from us (pension etc), you may be offered access to ZIO, our web portal.

ZIO is our customer portal. It gives an authorised user a window to view Zurich financial records about their individual pension plan activities and to issue requests to switch between pre-authorised funds. It will also offer the ability to make a request for a withdrawal from the pension plan subject to the authorisation form the pension trustee.

ZIO 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 session cookie containing a ZIO user authentication token, which persists for 15 seconds. It is possible to integrate ZIO into single sign-on environments using Security Assertion Mark-up Language (SAML) 2.0.

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®