ZURICH

Information Security at Zurich

Zurich's commitment to information security

At Zurich, protecting data and safeguarding confidential data of all our stakeholders is a top priority. Our approach to information security is based on three key focus areas:

Maintaining a **multi-layered security strategy** that considers people, processes, technology and data.

Employing a **risk-based approach** that considers external and internal risks, looking at past, present and future threats.

Addressing the **human element** of cybersecurity with awareness and education activities for customers, employees and business partners.

Information Security at Zurich

Zurich maintains a global information security framework that includes Group policies and processes regarding data and information security and the usage of IT equipment and assets. This covers, for example, the use of email, social media, removable media, physical security, etc.

Zurich's Group Chief Information Security Officer (GCISO) sets the overall strategy and security roadmap for the Group. The GCISO ensures that employees have the required security skills and knowledge and that regular forums track progress and ensure alignment across the organization. The GCISO reports to the Group Chief Information and Digital Officer who is a member of the Executive Committee reporting to the Zurich Group CEO. The Group Chief Information and Digital Officer is responsible at the Group Executive Committee for information/cyber security.

Zurich's Group Risk Management, Group Compliance, and Group Internal Audit functions provide independent challenge, analysis, advice, monitoring and assurance on cyber-risk matters and contribute to the overall strengthening of a risk-aware culture on information security and cyber-risk issues. External audits, regular third-party maturity assessments, and targeted deep dives are part of the overall assurance framework and strategy.

All Integrity Concerns are reviewed by a Triage Committee comprised of representatives from Compliance, Human Resources and Legal.

Zurich's Group Cyber Security function has a regional and local presence that allows it to proactively address the rapidly-changing nature of cyber and information security risk. The function has dedicated teams that perform key supporting roles in areas such as application security, business information security, cyber incident response, cyber threat operations and detection, information security governance, information security strategy, information security education and awareness, penetration testing, threat intelligence and vulnerability management.

Our information security policy is reviewed at least once annually, with standards and guidance updated every other year, or more frequently as necessary. Exceptions to policies or standards must be approved by senior management and are overseen or challenged as needed by the Group Cyber Security.
Our approach to information security and covers the following areas: Data Classification and Ownership, Access Control, People and Physical Security, Network and Device Security, Security Operations, System and Software Development Lifecycle Management, Disaster Recovery and Third Parties and Cloud Services.

Data Classification and Ownership

We take data security seriously. All our information is carefully classified based on sensitivity, ensuring appropriate handling and protection. Personal data is treated with the highest level of confidentiality, adhering to global data privacy standards. Learn more about our commitment to data privacy here.

Access Control

At Zurich, access to information is managed based on roles and requirements, following the principle of least privilege. We use advanced identity and access management systems, ensuring secure and unique user access. Administrative access undergoes strict approval and regular review, with enhanced security measures in place. Remote access is limited to approved users, secured through multi-factor authentication and zero trust principles.

People and Physical Security

We ensure that all employees and third-party suppliers undergo appropriate screening as part of our recruitment process. All staff are required to complete mandatory training in areas such as data security, privacy, and our code of conduct, with regular updates and targeted training for specific roles.

Our offices are secured with access control systems, and sensitive areas, e.g. data centers, have additional physical and technical access controls in place. Compliance with security policies is mandatory for all employees, and violations may lead to disciplinary action. We maintain an inventory of physical IT assets to ensure proper management and protection.

Network and Device Security

Zurich employs a multi-layered approach to network security, including firewalls, intrusion protection, and regular vulnerability assessments. Our network architecture is consistently reviewed and updated to ensure maximum protection.

We centrally manage and secure workstations, servers, and mobile devices using antivirus software, access controls, data loss prevention, and encryption. Approved mobile devices are protected through enterprise mobile management solutions and conditional access policies.

Internet access is managed through secure gateways, and Wi-Fi connections require two-factor authentication. Guest Wi-Fi is segregated from our corporate network to ensure security.

We have a robust process for vulnerability management and patching of servers and applications. Data transferred outside Zurich's network is encrypted, and internal data storage uses advanced security techniques, including encryption and physical protection.

Security Operations

The Zurich Cyber Fusion Center conducts regular scanning and auditing of our network and systems to ensure security. We have a structured process for managing, responding to, and reporting cyber and data incidents. Our operational response framework, reviewed periodically, covers security incidents and disaster recovery scenarios. We maintain 24/7/365 support for security incidents globally.

Our change management process ensures that technical changes are handled efficiently to avoid incidents and improve service quality. All changes are governed and audited by a change approval board to maintain operational excellence.

System and Software Development Lifecycle Management

We follow a rigorous development methodology for system changes and developments. All changes are first developed and tested in non-production environments before being moved to production through a controlled process, ensuring segregation of duties.

We prioritize security throughout the software development lifecycle, conducting thorough testing for vulnerabilities, including code reviews and penetration testing. Any discovered vulnerabilities are promptly addressed to ensure the highest level of data security.

Disaster Recovery

Zurich maintains a comprehensive set of business continuity plans that cover all critical aspects of business operations; including people, process and system accessibility. Zurich is dedicated to regularly test and exercise its business continuity to ensure operational resilience.

IT disaster recovery exercises for critical applications are conducted on an annual basis. Disaster recovery capacity allows for full recovery of the production environment in an affected primary data center.

Third Parties and Cloud Services

Zurich maintains a stringent supplier assurance and governance framework to ensure that third parties and business partners comply with our security and data privacy standards. Zurich maintains a stringent supplier assurance and governance framework to ensure that third parties and business partners comply with our data security and data privacy standards. This includes rigorous due diligence and strict requirements for data handling and security, and a dedicated cloud governance process.

Our dedicated primary and recovery data centers are located globally, and we also leverage public and private cloud services, such as AWS and Microsoft Azure, for application and data hosting to support many of our business services.

ZURICH®

Zurich Insurance Group | Group Compliance
Mythenquai 2, 8002 Zurich, Switzerland