Zurich applies multiple layers of protection to secure information assets

Zurich's approach to protecting own and client assets is risk based and comprehensive

Policies, Procedures and Standards

The Zurich Risk Policy, applied across the Group, lays down the Group´s risk management principles. There is a dedicated section on Information Security supported by detailed policy manuals, guidelines and standards including those for data handling and classification of assets and information. Technical standards define detailed measures which should be in place across the Group. Those policies, procedures and standards are subject to a variety of control attestation work and are factored in as part of ongoing activities, may this be within the area of IT infrastructure, applications and projects.

Restricted Access - Need to Know Principle

Access to assets and information is granted on a need to know basis and is subject to approval and periodic re-certification as appropriate. Processes exist to ensure timely removal and change of access rights when required.
The use of high privileged accounts is restricted and subject to enhanced logging and monitoring arrangements.

Vendors and Third Parties

Suppliers are subject to due diligence based on the classification of data they handle. Related risk assessments are performed by security specialists, legal/privacy and risk functions. Data protection clauses are included in all contractual arrangements.

Data Protection

Zurich has a multi-level defense architecture for protection of our core infrastructure components, servers and workstations against information security related events such as cyber attacks. Technical definitions are updated on a continuous basis. The infrastructure is subject to continuous vulnerability scanning and monitoring. Vulnerabilities are remediated as a priority given their severity and urgency, as assessed by our security experts.

Securing the Human Element

Employees are provided mandatory security awareness training annually and awareness is tested through campaigns. Confidentiality agreements are included in employee contracts.