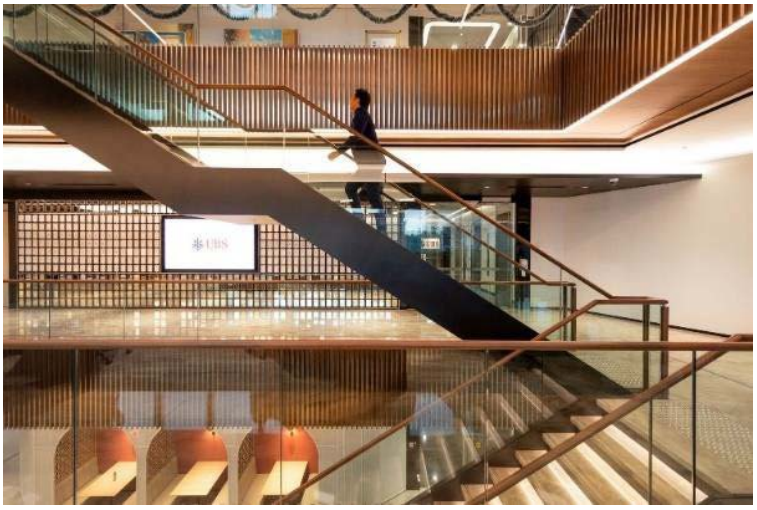
Cybersecurity, information security and data privacy at UBS

At UBS, the safety of our clients' assets and data is a top priority. As cyber threats to data increase in volume and sophistication, we continuously focus resources and investments on critical cyber and information security capabilities, with specialist teams working to safeguard your banking data, commercial information and financial assets.

UBS employs a multilayered and risk-based approach to maintain the confidentiality, integrity and availability of clients' personal data in a changing digital landscape. By embedding security and privacy into operations, we not only protect stakeholders but also contribute to the development of global standards and demonstrate leadership in shaping a sustainable and resilient financial system.



1. Our approach to information security

As a firm, UBS operates in accordance with industry standards in an evolving and increasingly complex environment. Our principles and policies reflect our commitment to appropriate security standards in how we use data and information, as well as how we develop and deploy technological solutions. Our cyber and information security (CIS) program is designed to identify, prevent, detect and respond to CIS events, with the goal of maintaining the integrity and availability of our technology infrastructure and the confidentiality and integrity of our information.

Policy

The firm has developed, issued and implemented a comprehensive written CIS policy suite that is applicable to all system infrastructure, applications, and firm users. The policy covers the governance model and roles and responsibilities as well as specific protocols and standards for topics, including, but not limited to, user identification, passwords, data encryption and system security. The policy is approved by the firm's senior management on a regular basis and is available internally to all UBS employees and consultants. Employees are required to review policies and affirm compliance on an annual basis.

2. Our approach to data privacy

We are committed to protecting data disclosed to us, with comprehensive measures (relevant controls, processes and policies) in place for the protection of personal data. We have also introduced organizational and technical security measures, underpinned by an operational risk and control framework, to safeguard personal data in accordance with applicable laws and regulations.

Our data protection policy framework covers the standards we commit to when processing personal data. The policy is reviewed annually and updated as appropriate, following the firm's general policy change framework.

The Group Data Protection Office, part of Group Compliance, Regulatory & Governance (GCRG), takes measures such that the firm processes personal data and responds to data subject rights exercised by individuals (including clients and employees) in line with applicable data privacy laws and regulations. Internal and external audit function assessments are in place to monitor compliance.

Any collection and processing of personal data by the firm in the context of the relationship with its clients is limited to what is stated in the firm's Client Privacy Notices, available on the firm's website. These outline the rights of individuals under applicable law, such as data access rights, and how they can be exercised. Please refer to https://www.ubs.com/global/en/legal/privacy.html.

Our vendor management program includes cybersecurity and data protection reviews, requiring relevant third parties to have appropriate controls to meet the firm's policy requirements. Our expectations and requirements must be formally acknowledged through dedicated contractual annexes (including the supplier data privacy policy). Third-party services and processes are monitored on an ongoing basis.

Privacy is considered during the design, development and deployment of new products, processes or services, with operational privacy review and data protection impact assessments (DPIAs) as applicable, so that data protection principles are considered from the start (privacy by design). In addition, by default personal data is processed with a privacy friendly setting (privacy by default).

Technical and organizational measures

Appropriate technical and organizational measures are implemented to keep personal data confidential and protected against accidental, unauthorized or unlawful destruction, and loss, alteration, disclosure or access. We use layered firm-wide controls to prevent and detect cyberattacks and data breaches.

Access rights are defined for information assets, and IT systems and applications enforce authentication. We maintain approval processes designed to prevent unauthorized access, and access to data is protected through control mechanisms following the need-to-know principle and revocation when no longer required. Where applicable and required, de-identification solutions are used for some specific use cases of sensitive client data. Users with highly privileged access are subject to additional vetting requirements as well as closer supervision, such as enhanced monitoring, more frequent background checks, block leave, segregation of duties and more frequent entitlement reviews.

Data is encrypted commensurate with its information security classification. Data-breach-prevention processes, such as blocking of communication and proactive remediation of misplaced data in unprotected areas, are in place.

Data handling

Data is processed for specific and explicit purposes (purpose limitation) and is adequate, relevant and not excessive (data minimization). Other key principles include that data subjects are informed of how their personal data is processed (fairness and transparency) and that it is not processed for longer than necessary for the given processing purposes (storage limitation). UBS has implemented processes to respond to data subjects exercising their rights, while adhering to applicable legal requirements.

Where a vendor has access to, processes or stores UBS data, additional data privacy requirements and controls may be specified. Non-disclosure agreements are mandated for third parties that have access to the firm's premises or data.

We are subject to complex and frequently changing laws and regulations governing the protection of client and personal data, such as the EU General Data Protection Regulation, depending on the jurisdiction. We communicate our client data use to clients and seek consent for data use as required by applicable regulations. In these communications and where relevant, we endeavor to be clear around what this consent means, and which use cases do not require consent, for example compliance with legal and regulatory obligations. We provide reasonable options for clients to be able to revoke this consent as applicable.

The Group Data Management Office, part of the Group Operations and Technology Office (GOTO), works with partners across UBS to provide robust governance over the collection, propagation and quality of the firm's data.

Data ethics

Our Data Ethics Policy outlines UBS's data ethics principles and requirements. These are considered during the design, development and deployment of new products, processes, or services for both input and output data.

Data ethics requirements include the following: human agency and oversight, technical robustness and safety, data privacy, explainability, diversity, non-discrimination and fairness, social and environmental wellbeing, accountability. They apply for the use of (i) AI, including machine learning and/or (ii) data analytics when processing personal data and/or other client data.

3. Governance and standards

Our Board of Directors (BoD) and the Group Executive Board (GEB) recognize that cyber and information security capabilities and data privacy are critical in protecting the firm and fostering an appropriate risk management culture. The BoD Risk Committee and the GEB oversee the CIS program through regular reviews and reporting and are part of the escalation chain for major and critical cyber incidents.

The Cyber and Information Security Committee (the CIS-C) is the primary decision-making body with oversight of and accountability for the Group-wide CIS program. The committee meets monthly and serves as a platform for interaction across all business divisions, Group functions and the three lines of defense for the identification and effective governance of CIS strategy, risks and regulatory obligations. The CIS-C governance structure is intended to streamline decision making and, where necessary, escalation to the BoD and GEB.

We follow the three-lines-of-defense model.

- The Group Operations and Technology Office (GOTO) establishes the policies and procedures designed to safeguard our information systems and the information those systems collect and process. The business divisions, together with GOTO, are then responsible for implementing those policies and procedures as part of the first line of defense.
- Group Compliance, Regulatory & Governance (GCRG) leads the second line of defense, by convening and consulting with additional control functions to provide independent oversight, challenges the first line's cybersecurity framework and implementation, and evaluates the design and effectiveness of individual security controls on an ongoing basis.
- As the third line of defense, Group Internal Audit conducts independent reviews and validates the first-line and second-line processes and functions.

Our Cyber Assurance Testing service provides testing and assurance of the firm's cyber security control functions through simulating the continuous evolution of tactics, techniques and procedures of real threat actors, based on their motivation, intent and attack capabilities, against (where possible) the firm's live infrastructure. We employ vulnerability assessments, penetration testing and red-teaming engagements based on specific threat scenarios that simulate tactics, techniques and procedures that might be used against our systems, as mandated by our policies. This includes testing by internal and external red teams.

The firm understands the importance of maintaining a robust security posture and adhering to industry best practices. The CIS program is aligned to industry standards such as ISO 27001 and the NIST Cybersecurity Framework, as well as standards mandated by regulators and local laws in the jurisdictions in which we operate. Our cyber and information security program leverages administrative, technical and physical safeguards, aligning with the Cyber Risk Institute (CRI) Profile, a cybersecurity framework tailored for financial institutions.

UBS is extensively audited each year by our external audit firm and has an independent internal audit function that continuously audits the UBS control environment. Both audit processes include regular examination and risk assessment of the firm's cyber and information security controls, technology controls, governance and frameworks, and general controls.

4. Training

All UBS staff, including the external workforce, receive appropriate CIS awareness and global data protection training, commensurate with their roles, responsibilities and level of access. We run a comprehensive, Group-wide education and awareness program, including addressing risks related to CIS. The program features mandatory computer-based training modules (recurring, and requiring exam completion), newsletters, and global and targeted awareness campaigns to all staff who have access to UBS systems. Additional educational campaigns, covering subjects such as phishing, malware infections, social engineering, tailgating, and data classification and leakage, are deployed several times per year. All UBS staff also undergo mandatory training on data privacy.

In addition, the BoD members receive periodic updates from the Group Chief Information Security Office (Group CISO) on key cybersecurity threats and incidents across the globe and industries, and the Risk Committee regularly organizes education and training sessions, including cyber exercises, for all BoD members.

5. Enforcement

Our Code of Conduct sets out the principles and behaviors that define our ethical practices and the way we do business. Any violation, whether it is of our Code, UBS policies or external laws, rules or regulations, may result in disciplinary action, up to and including dismissal. This includes information security incidents. Also, employees are, as part of their year-end performance rating, evaluated on their integrity. This includes doing the right thing, self-declaring incidents and issues, adhering to policies, challenging the status quo and raising their hand when things are not right (including potential security threats), and collaborating across teams, departments and divisions.

6. Threat intelligence and monitoring

We systematically gather threat information and monitor threat alerts from external sources. Our cyber-threat intelligence team analyzes such information and uses it to enhance existing defense capabilities, to respond to identified threats and to adjust our cybersecurity strategy where needed.

The Cybersecurity Operations Center is responsible for providing 24/7/365 real-time monitoring, detection and response capabilities for cybersecurity threats and attacks.

Furthermore, our Group-wide incident-handling process enables any UBS person to report incidents and data breaches. Additionally, we encourage employees to report any issues and incidents as per the incident-handling process, or to their line managers. Any compliance incidents can also be escalated through the whistleblowing process, which encourages individuals to raise concerns and challenge poor practice or behavior. An individual can report any concerns, including anonymously, through various established reporting mechanisms.

On a quarterly basis, the BoD receives reports on the performance of cybersecurity risk appetite metrics, including metrics on vulnerabilities and third-party cybersecurity risks and incidents, and is notified promptly if a Board-level cybersecurity risk limit is breached.

7. Incident response

UBS's incident response program includes procedures to notify impacted clients about incidents, where required, in line with the obligations stipulated in their respective contracts and in accordance with any applicable laws and regulations. Procedures include responding to, and escalating, cybersecurity and other system availability incidents. Our deployed security measures are designed with the objective to isolate and contain threats that are detected to allow for effective incident response and analysis. We also extend these processes to cover adverse information security events that take place at third parties but have relevance to UBS's information.

Our cybersecurity and data confidentiality contingency plans include event playbooks and escalation procedures designed to support a structured assessment of potential incidents and timely escalation and reporting of incidents based on the assessed potential impact. Incidents assessed to have the potential to adversely affect our critical operations are subject to mandatory management notification. If assessed as potentially significant, cybersecurity and data incidents are managed under

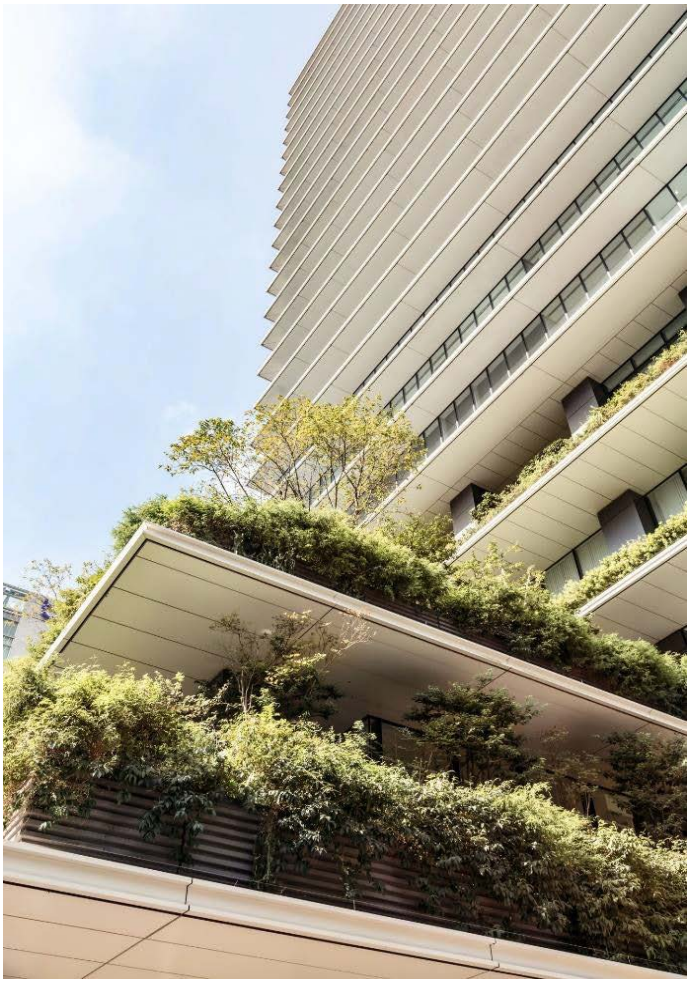
our crisis management framework, which provides pre-established cross-functional task forces for incident management, appropriate and timely regulatory, market and client communications and robust oversight by management, with escalation frameworks to inform and provide oversight by the GEB and the BoD. These plans are exercised regularly (at least once per year) using scenarios derived from the current threat landscape to verify that the response plans are appropriate, assess our readiness to manage and respond to such an incident, and adjust our plans and programs accordingly based on lessons learned.

8. Business continuity and resilience

The firm's Business Continuity and Resilience (BCR) framework is designed to limit disruptions ranging from standard operational interruptions to severe but plausible events, including CIS events, that could impact UBS's business activities, markets, clients, and infrastructure. Well established business continuity, enhanced operational resilience, and crisis management procedures and policies are in place in order to meet recovery objectives. The framework supports UBS's adherence to regulatory requirements and management of risks that could create undue exposure, whether financial or non-financial.

The BCR program covers all UBS business units and locations and applies readiness and response plans against a standard set of impact scenarios: loss of building, loss of critical technology, loss of critical third party, or unavailability of staff.

The BCR framework incorporates a range of recovery plans, which are reviewed annually. These plans provide a structured approach for the continuation or resumption of activities. The framework integrates periodic testing of crisis management, recovery solutions and systems to validate whether work may continue as planned during a major operational incident or event. Disaster recovery tests are conducted on a regular basis, where applicable.



Disclaimer: The statements made in this document have been made in good faith based on an appropriate level of due diligence. Given the dynamic nature of cybersecurity, information security, data protection, and their respective regulatory frameworks, the information must be understood to speak to the time it was provided and current as of the date of publication shown in the footer. This document has been provided for your information and does not constitute a representation or warranty by UBS. Neither UBS nor any of its directors, officers, employees, or agents accept liability for any loss or damage arising out of reliance on this information.