UBS

Global Supplier Policy

Audit Policy

WHY

To provide us with the information and oversight to help us meet our legal and regulatory obligations and ensure compliance

WHEN

Whenever you provide any of the following:

1. Outsourced Services;
2. BCM-Critical Services/Products;
3. SOX Relevant Services/Products; or
4. any Products or Services that are regulated by a Regulator of UBS.

WHAT to know about HOW to comply

1. Scope of audit

- You must grant (or, in the case of your Subcontractors, procure for) the Auditors the right to access any of your, your agents' or your Subcontractors' premises, personnel and relevant records (including devices, systems, networks, information and data used for providing the Services) as may be reasonably required in order to:
  - comply with any regulatory obligations or any legally enforceable request by a Regulator;
  - verify that you are complying with the terms of the Agreement (including any applicable Policies)that you are providing the Services in compliance with any Applicable Laws and Service Levels;
  - inspect any of our assets in your possession or control (including any IP Rights, UBS Data or UBS's Confidential Information) and the integrity, confidentiality and security of the same; and
  - identify suspected fraud or material accounting mistakes.
- You must provide Auditors with reasonable co-operation and access in relation to each audit.
- The Auditor's review rights will include, among other things, the right to review:
  - documents or information evidencing performance of the Services;
  - your risk management processes;
  - your information security and your physical, technical and administrative controls;
  - your disaster recovery and Business Continuity Plans,
  - any interdependencies in your supply chain and the operational resilience of your supply chain;
  - internal or external audit reports (e.g. ISO 27001, SOC 2 type 2, PCI DSS, etc.) and penetration test reports which have been completed by any independent bodies (these may be edited to restrict our access to your Confidential Information relating to other clients);
  - if applicable, your compliance with the Subcontractor Policy and any Subcontractor's compliance with any obligations relating to Subcontracted Services.
- You acknowledge that our regulated financial services clients may also be required to audit you in accordance with Applicable Laws, and that the rights in this Audit Policy extend to those clients (or their regulators or appointed auditors).

2. Conducting audits

- All audits will be performed in accordance with accepted national and international audit standards.
- When performing audits in multi-client environments, we understand that care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated, and we will endeavor to work with you in that regard.
- We will, where appropriate, consider performing pooled audits organized jointly with your other clients, to use audit resources more efficiently and to decrease the organizational burden on you and your clients.
- Before conducting any on-site visit or any physical audit, inspection or monitoring, we or the Auditors will provide reasonable notice to you, unless:
  - the audit arises from an emergency or crisis situation, a suspected act of fraud or a Security Breach;
  - the audit is required by a Regulator or is necessary to fulfil any regulatory obligation and it is impracticable or impossible to give reasonable notice;
  - such notice would render the audit ineffective.
- You will bear your own costs and expenses incurred in respect of any audit or inspection, as we will bear our own costs, unless a material default or non-compliance is identified, in which case you will reimburse our reasonable costs and expenses incurred in conducting the audit or inspection (including those of our Auditors or other third-party advisers).

3. Remediation activities

- If any audit or other inspection by any Auditor finds any non-compliance with any Applicable Laws, a Regulator's request, or the terms of the Agreement, including any applicable Policies, whether by you or on your behalf, you must promptly take all necessary steps to remediate the non-compliance.
- You must implement any other reasonable recommendations made by the Auditor within a reasonable timeframe or, if applicable, within the timeframe specified by the Auditor.

4. SOX Relevant Services/Products

- If you are providing SOX-Relevant Service/Products,
  - you shall put in place (or have put in place) appropriate

controls, including controls relating to IT applications, supporting infrastructure or IT processes (e.g., Cloud Services, data center, helpdesk, etc.). These controls and any control deficiencies must be reported in a SOC 1 Type 2 report (or equivalent report) as described in section (i) below.

- you shall conduct (or have conducted), at least annually and at your own expense, a financial reporting audit pursuant to:
  (i) SSAE No 18 Systems and Organizational Service Organizational Controls (SOC1) Type 2 standard for Services/Products provided directly or indirectly to UBS Group recipients that are established in the United States, and
  (ii) the International Standards for Assurance Engagements (ISAE) No 3402 standard for Services/Products provided directly or indirectly to all other UBS Group recipients,

  and promptly provide the results of such audit(s) to UBS.

5. Survival

- This Audit Policy will survive termination or expiration of the Agreement.