**Summary of Bumble's Information Security Policy:**

The Bumble Inc. ("Group") Board of Directors and Executive Management of the Group are committed to preserving the confidentiality, integrity, and availability of all information assets throughout the Group in order to protect and maintain its competitive advantage, cash flow, profitability, legal/regulatory/contractual compliance, as well as its commercial image and reputation.

As part of that commitment, the Group has implemented an Information Security Management System consisting of an Information Security Policy which aims to reduce risks associated with confidentiality, integrity, and availability to its information assets. The policy is applicable to all individuals and third parties doing work under the Group's control, and is intended to be an enabler for information sharing whilst reducing risk arising from the use of such information assets and associated technologies to acceptable levels and tolerances.

Fundamental to the policy are:

- Acceptable Use;
- Access Control;
- Cryptographic Controls;
- Data Backup;
- Incident Response;
- Information Disposal and Destruction;
- Information Classification;
- Information Transfer;
- Malware Protection;
- Password Composition and Management;
- Physical Security;
- Protection of Personally Identifiable Information;
- System Development, Configuration, and Deployment;
- Supplier Relationships;
- Teleworking; and
- Vulnerability Management

Control objectives for each of these areas are supported by more specific documents that align with the top-level Policy.
The Information Security Management System is subject to continuous improvement, policy documents are reviewed in response to changes in the threat environment and at least annually.