# ACCESS CONTROL POLICY (TIER 1)

1 MBP Pvt Ltd controls access to information on the basis of business and security requirements.

2 Access control rules and rights to applications, expressed in standard user profiles, for each user / group of users are clearly stated, together with the business requirements met by the controls, in ISMS-C DOC 9.1.2.

3 The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

4 The access rights to each application take into account:

a) The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the [systems and] network(s).

b) Data protection (Data Protection Act 1998, UK) and privacy legislation and contractual commitments regarding access to data or services.

c) The ‘need to know’ principle (i.e. access is granted at the minimum level necessary for the role).

d) ‘Everything is generally forbidden unless expressly permitted’.

e) Rules that must always be enforced and those that are only guidelines.

f) Prohibit user initiated changes to information classification labels (see control section 8.2 of the Manual).

g) Prohibit user initiated changes to user permissions.

h) Enforcing rules that require specific permission before enactment.

i) Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

5 MBP Pvt Ltd has standard user access profiles for common roles in MBP Pvt Ltd (see ISMS-C DOC 9.1.2).

6 Management of access rights across the network(s) is and in line with ISMS-C DOC 9.2.3.

7 User access requests, authorisation and administration are given upon the approval received from the respective departments head.

# ACCESS CONTROL POLICY (TIER 1)

8 User access requests are subject to formal authorisation, to periodic review (see control section 9.2.5 of the Manual) and to removal (see control section 9.2.6 of the Manual).

***Document Owner and Approval***

The *Chief Information Security Officer* is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff.

This policy was approved by the Board of Directors on [date] and is issued on a version controlled basis under the signature of the Chief Executive Officer (CEO).

Signature: Date:

**Change History Record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | Initial issue | Zamir Shaikh | 24th July 2024 |
| | | | |
| | | | |