INFORMATION SECURITY POLICY

INFORMATION SECURITY POLICY

Founded in 2023, MBP Pvt Ltd is a lead and demand generation firm with focused expertise in helping companies who are in constant search of business leads to make their marketing campaign a success. Leveraging on their experience since 2020 at over 150 projects across multiple clients, MBP Pvt Ltd has been able to continuously innovate in the formulation and delivery of relevant services to both users and providers of technology.

The Management of MBP Pvt Ltd is committed to ensuring the Information Security of the company's confidential data and critical technology infrastructure. The scope of this Information Security Management System ('ISMS') includes the Information Systems, Information Processing Facilities, and Operations that are involved in MBP Pvt Ltd's lead generation activity.

ISMS covers the Confidentiality, Integrity, and Availability of data in various forms such as software code, QMS (Quality Management Services), delivery methodology, internal operational data, employee data, and client data.

The ISMS covers the entire lifecycle of the client's data (raw data, software code, processes, etc) from the time it is received by MBP Pvt Ltd, and then processed, stored, transmitted, backed up, and finally terminated.

The scope of ISMS also applies to all the departments of MBP Pvt Ltd, Pune namely: Delivery, IT Services, Finance, HCM (Human Capital Management),and Office Administration. Non Critical data processing and sanitization is done either physically at the following location i.e. Office No 1 & 2, Arihant Avenue, Divya Nagar, Wanwadi, Pune, Maharashtra 411040, INDIA.

For, third-party vendors, an SLA and NDA which includes Information Security as a requirement will be signed, monitored and reviewed regularly.

The objective of the ISMS is:

- To give assurance to the management, stakeholders and clients of the security of data in MBP Pvt Ltd.
- Raise awareness of the organisation's employees about the importance of information security.
- Strengthen the internal controls for information security with a high level of accountability.
- Ensure and demonstrate due diligence to various legal and contractual compliance obligations.

Mr. Zamir Shaikh (Chief Information Security Officer) has been nominated by the Management to be the ISMS Head who will be responsible for all activities of the ISMS.

INFORMATION SECURITY POLICY

The organization's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of ISMS. The risk assessment, Statement of Applicability and risk treatment plan identify how information-related risks are controlled. The ISMS committee leader is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Information Security Manual and are supported by specific, documented policies and procedures.

All employees of the MBP Pvt Ltd working with research data and other third party vendors identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All staff, and certain external parties, will receive appropriate training.

The ISMS is subject to continuous, systematic review and improvement. MBP Pvt Ltd. has established an ISMS council chaired by the ISMS Committee Head and includes personnel from Delivery, IT services, HCM, Admin, Finance to support the ISMS framework and to periodically review the security policy.

The controls implemented as a part of ISMS are in line with ISO/IEC 27002:2005 requirements. Contractual obligations fulfillment is also a part of the control requirements of the ISMS.

The organization is committed to achieving certification of its ISMS to ISO27001:2022

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan at least annually.

ISO/IEC 27701:2019 (PIMS- Privacy Information Management System)

MBP Pvt Ltd has extended the scope of ISMS with additional security measures related to ISO/IEC 27701:2019 (PIMS- Privacy Information Management System). The following standard has been enforced to ensure Privacy and data protection is implemented in accordance with GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) and other similar regulations.

INFORMATION SECURITY POLICY

In this policy, "information security" is defined as:

preserving

This means that management, all full time or part-time staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in section 13 of the Manual) and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in the organization's disciplinary policy. All staff will receive information security awareness training and more specialized staff will receive appropriately specialized information security training.

the availability

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network identified as part of the scoping work for section 1 of the Manual must be resilient and the organization must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

confidentiality

This involves ensuring that information is only accessible to those authorized to access it and therefore to preventing both deliberate and accidental unauthorized access to the organization's information and proprietary knowledge and its systems including its network(s), website(s), extranet(s), and e-commerce systems.

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorized modification, of either physical assets or electronic data. There must be appropriate contingency including for network(s), e-commerce system(s), web site(s), and extranet (s) and data back-up plans, and security incident reporting. The organization must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of the organization including but not limited to computer hardware, data cabling, telephone systems, wireless, filing systems and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, web site(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs as well as on CD ROMs, floppy disks, USB sticks, back up tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

of the organization

the organization and such partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS.

INFORMATION SECURITY POLICY

The ISMS is the Information Security Management System, of which this policy, the information security manual ("the Manual") and other supporting and related documentation is a part, and which has been designed in accordance with the specifications contained in ISO27001:2022

A SECURITY BREACH is any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of the physical or electronic information assets of the Organization.

The Director is the Owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements in clause 5.1.2 in the Manual.

MBP Pvt Ltd is committed to achieving certification of its ISMS to ISO27001:2022.

The ISMS is the Information Security Management System, of which this policy, the Information Security Manual ('the Manual') and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2022.

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a breakdown in the availability, confidentiality or integrity of the physical or electronic information assets of MBP Pvt Ltd.

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 requirements in Clause 5.1.2 in the Manual.

A current version of this document is available to all members of staff and is published. It does not contain confidential information and can be released to relevant external parties.

Signature: Date:

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Azim Shaikh	5th Nov 2024
2	Appointing ISO (Chief Information Security Officer) – Zamir Shaikh	Azim Shaikh	5th Nov 2024
3	Inclusion of PIMS 27001:2022	Azim Shaikh	5th Nov 2024