



Altria Consulting (Pvt) Ltd

Information Security Management System (ISMS)

Information Security Policy Statement

Document Number: Altria-ISMS-MN-005

Classification: Internal

Document Owner: Information Security Officer (IS Officer)

Version: 1.0

Effective From:

Document History:

Release Date	Revision No	Author(s)	Description	Reviewed & Approved By
08-Feb-2024	0.1	IS Officer	Initial Release	
	1.0	IS Officer	Approval and Publishing	Information Security Steering Committee

Contents

- 1. Purpose3
- 2. Distribution3
- 3. Information Security Policy Statement.....3
 - 3.1 About Altria.....3
 - 3.2 Information Security Policy Statement.....4

1. Purpose

The purpose of this manual is to provide information regarding the Business Processes and the Information Security Management System of Altria to interested parties of Altria.

2. Distribution

This is an internal document and can be shared with employees at Altria and intended parties determined by the Information Security Officer (IS Officer).

3. Information Security Policy Statement

3.1 About Altria

Altria is a consulting organization with a specialization in data analysis and ERP implementation and support. Information security is a collaborative approach in which clients and Altria both have their specific roles and obligations, within a framework of Altria's information security policy. Altria understands and accepts information security policy/terms in agreement with its clients and conducts business in conformity with it. Altria's Information security policy includes compliance with applicable data protection legislation in relevant markets/business scope.

Clients use ERP products licensed to them by the OEMs e.g. SAP. The terms of the license include the number of users and modules and the provision of cloud storage. Altria consults clients for customization of the business in the ERP and trains staff in the use of ERP. After the project is implemented, Altria gives support such as managing the functional changes, changes in databases, and applying OEM-provided patches for technical upgrades, in ERP with specific approval and authorization of clients in a mutually agreed manner.

Altria does not need nor does it have any access to the real data of clients. Client-provided data meant for testing purposes are their responsibility and are masked/ de-identified and do not represent real data. Releases after changes are subject to UAT (User Acceptance Tests) by clients. Every release is subject to configuration management. Altria is absolved of any responsibility for the real-time performance of ERP as it is not authorized nor does it deploy the ERP software and databases and changes into servers of clients, directly. Responsible personnel, change requests from clients, responses to them, and the manner/tool used for communication and service levels are decided and agreed upon between the parties concerned. Any changes in personnel and/or method of communication by parties are mutually agreed to prevent a risk of any unauthorized communication.

Altria under staffing services provides resource persons to work under the control of clients. In this model, Altria facilitates clients to select/nominate resource persons under the staffing agreement. Here, clients own the staff for all practical purposes and induct them into their information security policy and controls. Staff of Altria can be posted on site where they work in a client-controlled environment or can work remotely from the office of Altria, subject to agreement. The role of Altria

in remote working is limited by the provision of IT equipment, tools/methods used for communication (VPN or whitelisting of internal IPs), and office facility and address any concerns raised by clients.

Altria is also a reseller of Tableau and PowerBI. These are data analysis tools. The role of Altria is to facilitate clients in developing a dashboard for data capture and visualization. Here, Altria or its staff have no access to any real data of clients but data provided by clients are good only for demonstration and testing. The role of Altria is limited to developing scripts in Tableau/PowerBI and change requests. Altria presents a dashboard as a demonstration, for approval of clients. Clients can use the dashboard with real data. In doing this, Altria has no data risk of clients.

In rare cases, when clients require Altria to access real business data, clients have to first accept responsibility for their data risk. Data resides in client-controlled servers and Altria staff works in the client environment. Activities such as authorization, access control, and log of activity by staff of Altria are authorized and approved by clients.

Process owner for the product and services (e.g., SAP support) has a standard method and template that are used by each project manager to identify risks for a particular project with regard to customer requirements, requirement of resources, and timely delivery.

3.2 Information Security Policy Statement

- Altria Consulting is a leading organization in the country providing data analytics and Enterprise Resource Planning (ERP) consultancy services for customers locally and internationally.
- In providing these services Altria has access to customer's information systems but does not hold, collect or transfer any sensitive information of customers to the Altria side. The management of Altria is committed to protecting and safeguarding the information Altria has disclosed by implementing adequate protection mechanisms. In addition, Altria's management is also concerned with protecting Altria's own proprietary information and information systems including employee information which gives us, a competitive advantage against our peers.
- Keeping in mind the above goal, management has implemented an Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022 information security, cybersecurity, and privacy standards by continues improvement. The ISMS will also intend to comply with contractual obligations that Altria has with any stakeholder related to information security, legal requirements, and any regulatory requirements that may apply to us.
- Management of Altria has empowered the Information Security Steering Committee (ISSC) to implement the ISMS by analyzing information security risks that are applicable, determining suitable risk treatment options to mitigate the risks, and implementing appropriate controls covering people, processes, and technology.
- We are expecting the following objectives to be achieved through the ISMS:
 - Increase the information security posture of the IT environment that Altria utilizing;
 - Minimizing information security risks, by identifying, assessing, and determining appropriate treatment options for information security risks;

- Comply with legal, regulatory, and contractual obligations applicable to our business and the markets we operate in; and
- Increase the information security awareness of our employees and minimize information security breaches that may occur through them.

ISMS will assist Altria in raising confidence in the information security posture of our organization with different stakeholders.