Information Security Policy

1. Summary / Purpose

The purpose of this document is to demonstrate the Management Board's commitment to information security and to provide the over-arching policy statements to which all subordinate policies and controls must adhere.

2. Definitions

In this policy, as well as the related set of policies, that incorporate our ISMS (Information Security Management System), 'information security' is defined as:

Preserving

Preserving means that all relevant Interested Parties have, and will be made aware of, the responsibilities that are defined in their job descriptions, or contracts, and are expected to act in accordance with the requirements of the ISMS. The consequences of any contravention are described in the Code of Conduct. All relevant Interested Parties will receive information security awareness training, while more specialised resources will receive appropriately specialised information security training.

Availability

Availability means that information and associated assets should be accessible to authorised users when required and must therefore be physically secure. The environment must be resilient, and the organisation must be able to rapidly detect and respond to incidents or events that threaten the continued availability of assets, systems, and information.

Confidentiality

Confidentiality implies that information is only accessible to those authorised to access it. It also entails the prevention of deliberate and accidental unauthorised access to the information, proprietary knowledge, assets, and other systems in scope that belongs to the organisation and other relevant parties.

Integrity

Integrity involves safeguarding the accuracy and completeness of information and processing methods. This requires prevention of deliberate or accidental, partial, or complete, destruction or unauthorised modification, of either physical assets or electronic data.

Information and other relevant assets

The information can include digital information, printed or written on paper, transmitted by any means, or spoken in conversation, as well as information stored electronically. Assets include all information-based processing devices owned by the organisation or those of relevant Interested Parties, as well as BYOD (bring your own device) in scope, which process organisation related information.

Our organisation

The organisation and relevant Interested Parties that are within the scope of the ISMS have signed up to our security policy and accepted our ISMS.

3. Policy

The Board of Directors and management of Signify (Pty) Ltd located in Centurion, Gauteng, operates as a software development company specialising in Human Resource Management Software.

Signify is committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information, along with information-related assets, to meet the purpose and goals of the organisation as summarised in ISO 27001:2022 clause 4 - Context of the organisation.

Information and information security requirements will continue to be aligned with the organisation's business goals and will consider the internal and external issues affecting the organisation and the requirements of interested parties.

Signify's ISMS Objectives are outlined and measured in accordance with the requirements of ISO 27001:2022.

The ISMS is intended as a mechanism for managing information security related risks and improving the organisation in order to deliver on its overall purpose and goals.

The MS, including our approach to risk management, provides the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of an ISMS.

The approach taken toward Risk Assessment and Management, the Statement of Applicability and the wider requirements set out for meeting ISO 27001:2022, identify how information security and related risks are addressed.

The Management Review Board is responsible for the overall management and maintenance of the risk treatment plan, with specific risk management activity tasked to the appropriate owner within the organisation. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks, for example during special projects that are completed within the context.

Control objectives for each of these areas are supported by specific documented policies and procedures in the online environment that are aligned with the comprehensive controls listed in Annex A of the ISO 27001:2022 standard.

All employees and relevant Interested Parties associated with the ISMS have to comply with this policy. Appropriate training and supporting materials are available for those in scope of the ISMS. Furthermore, communication forums such as the ISMS communications group are available to ensure engagement on an ongoing basis.

The ISMS is subject to review and improvement by the Management Review Board, chaired by the Chief Information Security Officer (CISO) and has ongoing senior representation from appropriate parts of the organisation. Other executives / specialists needed to support the ISMS framework to periodically review the security policy and broader ISMS are invited in the Board meetings. These executives / specialists complete relevant work as required in accordance with the documented standard.

Signify is committed to achieving and maintaining certification of the ISMS to ISO27001:2022 along with other relevant accreditations to which the organisation has sought certification.

This policy will be reviewed once per annum, or whenever significant changes in the company occur, in order to respond to any changes in the business, its risk assessment, or risk treatment plan.