|  |  |
| --- | --- |
| [company name]  Information Security Policy | |
| Organisation | [company name] |
| Scope of policy | This policy applies to the business of [company name] wherever it is conducted, but based at the registered office. It applies to paid staff. |
| Policy operational date | X |
| Policy prepared by | X |
| Date approved by Information Officer | X |
| Policy review date | X |
| IntroductionPurpose of policy | The purpose of this policy is to enable [company name] to:   * Provide a framework for the management of information security; * Promote awareness of the importance of protecting [company name]’s information; * Identify information related risks; * Identify and report on unauthorised information access leakages or attempts to obtain information through unauthorised means; * Follow good practice for information security. * Comply with the relevant provisions of the POPI Act 4 of 2013, in particular Condition 7, sections 19 to 22. |
| Objective | The overall objective of the [company name] Information Security Policy is to ensure that safeguards for the protection of the Integrity, Availability and Confidentiality of Information Assets are established. |
| Secure environment | A secure environment is based on managing risk at an appropriate level. The security controls applied to an Information Asset should be commensurate with the magnitude of harm that would result from the loss, misuse, inability to access, unauthorised access to, or modification of the information in a system. |
| Information covered | Although the protection of automated information resources is emphasised, protection requirements will cover all Information Assets, including, but not limited to, physical, personnel, computers, networks, telecommunications systems, applications, data, faxes, paper repositories and any other media used to store or process information. |
| Information Classification | Information assets have varying degrees of sensitivity and criticality and some items may require an additional level of protection or special handling. A clearly defined Information Classification System will be used to define an appropriate set of protection levels, and communicate the need for special handling measures. |
| Policy Statement | [company name] will:   * Ensure that adequate Information Security Policies are implemented to enforce compliance to the accepted Information Security standard; * Ensure that information assets have a nominated owner to ensure the accountability of systems, equipment and information at all times; * Ensure that Identification and Authentication measures for access to information systems are implemented and maintained; * Ensure that responsibilities and procedures for the secure management and operation of information processing facilities will be established to prohibit unauthorised access, disclosure, duplication, modification, destruction, loss, misuse, or theft of information. * Develop a Business Continuity plan to reduce the disruption caused by disasters and security failures in order to allow critical systems to continue in the event that critical facilities and resources are not available. |
| Personal Information Security Measures | * Measures for protecting personal information in accordance with the Protection of Personal Information Act (POPI) will be established within the overall security management system. * In accordance with the act, appropriate, reasonable, technical and organisational measures will be established * The measures will established in order to prevent the loss or damage, unauthorised access and destruction to personal information. |
| Key Risk | [company name] has identified the following potential key risks, which this policy is designed to address:   * Breach of security by allowing unauthorised access to internal and external users e.g. sharing usernames/passwords; * Hacking attempts; * Virus attacks; * Information stored on mobile devices lost or stolen; * Lack of knowledge among employees regarding the importance of protection company information. |
| Business Continuity | Disaster recovery 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 and will be developed, and maintained. |
|  | |
| Responsibilities | Managing Director/CEO has overall responsibility for Information Security. This responsibility may be delegated to an Information Security Officer or Information Officer for the management of issues relating the controlling of access to information and privacy of information in terms of legal requirements as prescribed in the PAIA Act, PoPI Act and other related acts or regulations. |
| Information Security Officer has the delegated responsibility for all aspects of Information Technology security management, including planning, budgeting, monitoring and reporting and the co-ordination of control implementation. |
| Business Information Owners have the authority and responsibility to:   * judge the value and sensitivity of information and classify it in accordance with the relevant security policies, standards and procedures; * ensure that their business information is protected in accordance with the Information Security Policy; * authorise access to the information for which they are responsible; * assign custodianship for information; * specify controls in service level agreements and communicate the control requirements to the custodian and users of the information and obtain assurance from the custodian that control requirements are met; * develop business continuity plans; * monitor compliance with information security policies, procedures, standards and security measures, and record and report violations thereof. |
| Employees, Temporary Employees, Contractors and Third Parties who have access to the information belonging to [company name] are responsible for adhering to the various Information Security Policies, Standards and Procedures documents. They have an inherent responsibility for protecting information during the course of their daily activities. |
| Operators, which includes but is not limited to external parties such as Business Partners and IT Service Providers, who process information, in particular personal information, are responsible for adhering to the various Information Security Policies, Standards and Procedures documents, as well as the Conditions for Security Safeguards and Measures regarding information processed by the Operator. |