MASTERSTART

POPI Act & Information Security Policy

Rules and guidelines for the POPI Act and Information Security

MASTERSTART

Table of Content

MASTERSTART

1. Introduction

The purpose of this Information Security Policy is to establish and communicate the Executive Team's expectations for information security within the organisation, to ensure the security of sensitive information under MasterStart's custody or care and the ongoing secure operation of the business in order to protect the organisation, its systems, data, and resources, and to ensure shareholder value.

This policy applies to all business units in all markets in which MasterStart operates, and to all employees and independent contractors.

2. Information Security Background

MasterStart, as an organisation in the training and education sphere, relies upon sensitive information in the course of its business, and it is the responsibility of the organisation, its employees and partners to protect the confidentiality, integrity, and availability of that information.

Any compromise of the information under the care of MasterStart could cause harm to learners, employees, and business partners, and damage the reputation significantly. MasterStart could also be at risk of regulatory or legal sanctions should they not exercise their duty of care to protect that information.

Ultimately, the learners, employees and business partners of MasterStart trust their information and resources to be prioritised and looked after, as they continue to work with the organisation. This trust is repaid by defining and upholding security responsibilities.

3. Consequences of non-compliance

The MasterStart Information Security Policy is of great importance to the Executive Team.

Failure to comply with the Information Security Policy may result in disciplinary action or sanctions being taken against those in breach of this policy and its associated sub-policies, guidelines and standards.

Any employee that is found to be responsible for an event where a breach of information security occurs through negligence, or

non-compliance to the Information Security and/or relevant sub-policy policy, will be held fully accountable for the incident and subjected to the Disciplinary Code procedures of MasterStart.

Any person that has knowledge of a breach of information security and fails to report the incident for whatever reason, will be held fully accountable for the incident and subjected to the relevant Disciplinary Code procedures of MasterStart.

Any external third-party or contractor to MasterStart that is in violation of the policy, will be held accountable and contractual agreements will be subject to immediate suspension or termination, as per the discretion of the executive management.

Under this policy, all MasterStart employees and third-party contractors are obligated to report any security incident or breach, or suspected breach of information security immediately to their relative line manager/s, as well as the Information Security Officer of MasterStart. It is the subsequent duty of the Information Security Officer to investigate the incident, compile the breach report and if required, inform the relevant Information Regulator.

4. Policy Objective & Goals

The objective of information security is to ensure the business continuity of MasterStart and to minimise the risk of damage by preventing security incidents and reducing their potential impact.

The goal of the policy is to protect the organisation's information assets against internal, external, deliberate, and accidental cyber threats.

The Information Security Policy ensures that:

- Information and Data within the organisation receives appropriate levels of protection against information security threats.
- Appropriate levels of security are guided by a risk management framework that includes risk assessments that identifies the threats, the possible impact and the likelihood of the threats being realised.
- Confidentiality of information will be assured.
- Integrity of information will be maintained.
- Availability of information for business processes will be maintained

- Business continuity plans will be developed, maintained, and tested.
- Information security training will be available for all employees relative to roles and responsibilities.
- Legislative and regulatory requirements will be met and compliance with and adherence to applicable local and international regulations.
- All actual or suspected information security breaches will be reported to the Information Security Manager and will be thoroughly investigated.

Procedures are defined and implemented to support the policy, including malware and ransomware control measures, authentication mechanisms and continuity plans.

5. Policy Management & Governance

The Information Security Officer is responsible for maintaining the policy and providing support and advice during its implementation. The management team is directly responsible for implementing the policy and ensuring staff compliance in their respective departments.

Compliance with this information security policy is mandatory and a management framework will be established to initiate and control the implementation of information security within MasterStart to adhere to the security objectives as detailed in this policy and guided by the Security Charter.

To comply with legislation and to facilitate and manage the implementation aspects of this policy, the Information Officer (also referred to as the Data Protection Officer) for MasterStart will be the Managing Director or a duly authorised person according to the requirements of the Protection of Personal Information Act (POPIA) and the General Data Protection Regulation (GDPR). The appointed Information Officer will be duly registered with the Information Regulator as is and when required and will report to the Senior Management, or Board of Directors of the Company as may be applicable.

The role and responsibilities of the Information Officer/s will be included and be communicated in a formalised and documented job description.

MASTERSTART

6. Legal & Regulatory Requirements

MasterStart regards the safekeep of information as essential to the business and must therefore ensure that information is protected, and security safeguards are maintained in accordance with applicable laws and regulations.

MasterStart is committed to:

- Identify any legal or regulatory requirements which may impact the Information Security Policy.
- Ensure responsibilities for compliance with laws and regulations are assigned and understood.
- Establish governance practices which establish, resource, and maintain information security practices.
- Publish and maintain this policy and support information security standards to all personnel.

The following regulations are identified:

- Protection of Personal Information Act (POPIA)
- General Data Protection Regulation (GDPR)

7. Protection of Assets

The objective is to ensure appropriate controls are in place to secure MasterStart's information, as guided by regulations and legislations, and the risk profile, based on the value of the information to the business.

MasterStart is committed to the upkeep of an Asset Register by:

- Identifying information assets used within the organisation and assigning ownership.
- Ensuring that assets are classified and protected as per a classification framework.
- Ensure consideration of security risks are incorporated into project management and software development methodologies.
- Information assets are classified in accordance with the Information Classification Framework.
- Controls are implemented to ensure information assets are managed in accordance with the Information Classification Framework.

8. Management of Security Risks

In the management of our risk, the objective is to understand the security risks to our information assets and business operations, and to take precautions commensurate with the risks to the business.

MasterStart is therefore committed to:

- Define the risk appetite for the business per a Risk Management Framework.
- Ensure risk assessments are undertaken on a regular basis, are reported on, and managed.
- Undertake risk assessments annually, or as required by changes to the legal or regulatory environment.
- Implement and manage controls in line with the risk.
- Maintain a risk profile within the risk appetite and report and manage risks to the business.
- Implement security controls in accordance with MasterStart 's security standards and guidelines.

9. Access to Information

Our objective is to ensure only appropriate access to information assets and resources is provided to parties who require access, as per defined roles and responsibilities.

Commitment to:

- Authorise access to information assets only if there is a business requirement for access.
- Review access to information assets on a quarterly basis and remove those without a business need.
- Ensure the access authorised minimises risk of fraud or misuse.

Access Control Procedures will be in place to:

- Only provide access that has been authorised.
- Only provide access to information assets and resources using a uniquely identifiable method.
- Only provide access that supports segregation of duties, according to roles and responsibilities.
- Monitor the use of resources and assess future capacity requirements to ensure required system performance metrics are met now and into the future.

10. Incident Response

Our objective is to ensure that MasterStart has the capability to detect and respond to security incidents to prevent disruption to business activities, and reduce the risk of harm to MasterStart's partners, customers and personnel and any consequent reputational damage.

This is achieved by our commitment to:

- Develop and maintain an incident management framework to ensure methodical resolution of incidents.
- Implement security monitoring capabilities on all environments and systems hosting sensitive information.
- Resolve security incidents effectively.

11.Security Assurance

MasterStart is responsible to regularly provide proof to auditors, regulators, and third parties that information assets are protected.

Our objective is to validate that implemented security measures are functioning effectively and as expected, and we are able to report to relevant internal and external stakeholders.

MasterStart is committed to:

- Review information security policies and standards regularly (at least annually) to ensure their continuing relevance and effectiveness.
- Gather and maintain evidence of security measures that have been implemented within the organisation.
- Assess and report on compliance with relevant information security controls for all systems.
- Obtain independent assessments and testing of information security controls, and ensure remediation activities are undertaken of identified, unsatisfactory controls.
- Maintain appropriate contacts with external groups, forums and associations that deal with emerging cyber security threats.
- Ensure IT systems are regularly reviewed to ensure specific regulatory compliance.

12. Manage Third Party Risks

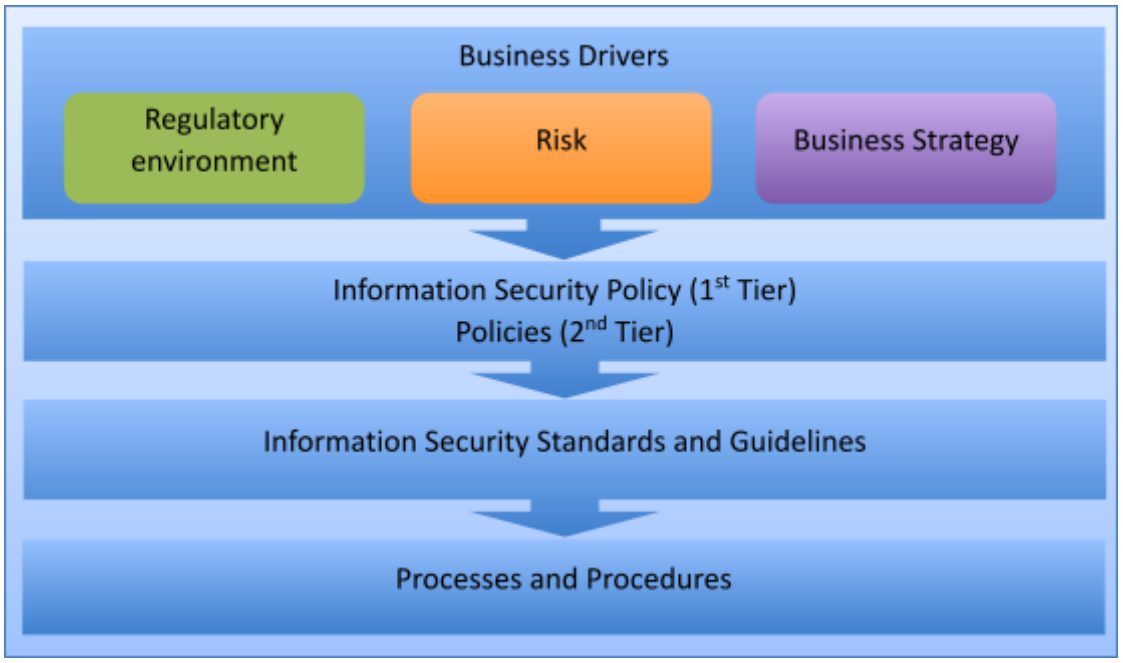
Our objective is to ensure our partners can be trusted to protect MasterStart's information assets under their care by managing our external stakeholders to reduce the risk of compromise of sensitive information.

We are committed to:

- Take accountability for the security of our external stakeholders.
- Ensure that all agreements with third parties include security provisions, the right to audit, and a requirement to report security incidents to MasterStart .
- Develop and maintain a process by which MasterStart can assess and report on information security controls of third parties.
- Evaluate and audit the compliance of third parties with relevant security standards and their ability to secure the information entrusted to them.

13. Information Security Framework

The following model depicts how the information security policy fits together with other information security framework documents and provides context on inputs into formulation for the security policy and associated documents.



The following Policies and Guidelines are utilised for implementation of the Information Security Policy:

- Data Privacy Policy
- Information Classification Policy

14. Security Exemptions

While the MasterStart Information Security Policy (and its associated Standards and Procedures) apply to all its employees as well as third parties with access to MasterStart's systems or information, there may be instances in which compliance with specific security requirements is not possible.

In these circumstances, the following steps must be followed:

Step	Description
Lodgement of Exemption Request	The relevant Business Unit is to identify activities which are unable to meet documented security requirements and request an exemption from the relevant requirement(s) by lodging a Security Exemption Request. The Exemption Request must be lodged with Management and needs to: 1. identify the specific security requirements that cannot be complied with; 2. the reasons for non-compliance;

	3. any mitigations that may be able to be implemented to compensate for the non-compliance.
Review of Exemption Request	Once the Exemption Request is received, the Information Security Officer or Security Manager will review it to consider whether granting the exemption: ● May impose unacceptable security risks; ● May otherwise unduly impact the ability of MasterStart to achieve its business objectives; ● Whether it is practical and possible to implement any mitigating actions in order to reduce the level of risk associated with the exemption, should it be approved. A LOW, MEDIUM or HIGH-risk rating must be assigned, depending on the level of severity associated with the exemption and include a recommendation as to the duration the exemption should last for prior to being reviewed.
Approval of Exemption Request	The Exemption Request must be forwarded to a member of the Executive Team (for HIGH RISKS) for approval. The relevant reviewer (the Security Manager or Executive Team member) must decide whether to approve the Exemption Request based on the information provided by the Security Manager. If approved, the approval must also include the duration for which the exemption remains valid.
Documentation of risks for approved requests in Risk Register	If the Exemption Request is approved, it must be ensured that the risk is documented in the Risk Register (only required for requests that are given a HIGH or MEDIUM risk rating).
Review of Approved Exemptions	Approved Security Exemptions must be reviewed annually by the to ensure that the granting of the Exemption still remains appropriate. If this is not the case, the Security Manager should notify the relevant Business Unit and forward to the Team Leader (for exemptions with a LOW or MEDIUM risk) or Executive Team member (for exemptions with a HIGH risk) for consideration as to whether the exemption should continue to remain valid.

MASTERSTART

Document Details

Document reference number	Information Security Policy V1
Document Title	Information Security Policy
Classification	PUBLIC
First release of document	01-11-2021
Issue date of document	01-11-2021
Next revision due	01-11-2024
Policy owner	Siyamthemba Kakaza