DATA PROTECTION POLICY
LAST UPDATED AUGUST 21st, 2024

A. INTRODUCTION

1. OVERVIEW

Massy needs to collect and use certain types of information with regards to individuals, companies and Service contractors whom they do business with. Personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

2. PURPOSE

The purpose of this policy is to describe how personal or confidential data must be collected, handled, and stored to meet the company's data protection standards. It also addresses the prerequisites for Massy Group companies to comply and operate within the laws of the country.

3. SCOPE

The data protection policy ensures that Massy Group companies adhere to the following:

a. Complies with data protection law and follows good practice.
b. Protects the rights of staff, customers and partners.
c. Is open about how it stores and processes individuals' as well as customer data.
d. Protects itself from the risk of a data breach.

B. POLICY

1. DATA PROTECTION LAW

The Massy Group intends to ensure that personal information is treated lawfully and appropriately. The principles of Data Protection as outlined in any laws and regulations that may exist in any country in which the Massy Group operates are listed below. Such principles have been drafted to cover, as far as possible:

a. Personal data shall be processed fairly and lawfully
b. Each Massy company is responsible for the information under its control.
c. The purpose for which the personal information is collected shall be identified by each Massy company.

d. Personal information shall not be kept longer than is necessary.
e. Personal information collected shall be accurate, complete and up-to-date as necessary for the purpose of collection.
f. Personal data must be protected with appropriate safeguards having regard to the sensitivity of the information collected.
g. All Massy companies must be in a position to make available the data collected on each customer to that customer, as well as any documentation regarding the company's policies and practices related to management of personal and confidential information.
h. All Massy companies must be able to disclose at the request of the individual or company all documents relating to the existence, use and disclosure of personal and confidential information, such that the individual can challenge the accuracy and completeness of the information.
i. Any information breach must be reported immediately on discovery to the employee's manager, the relevant ICT department manager, and the Group's most senior personnel responsible for Information and Cyber Security.

2. DATA PROTECTION RISKS

This policy helps to protect Massy from data security risks such as:

a. **Breaches of confidentiality** – this breach will be information being given out incongruously.
b. **Reputational damages** – the company could suffer damages if hackers successfully gain access to sensitive data.

3. DATA COLLECTION

When collecting data, each Massy company must ensure that the data collected is within the boundaries defined in this policy. This applies to data that is collected in person, or by completing an electronic form. When collecting data from customers all Massy companies must ensure the following:

a. That individuals clearly understand why the information is needed.
b. That individuals understand what the information being collected will be used for and what the consequences are should the individual decide not to give consent to processing.
c. As far as reasonably practicable, the individual is competent enough to give consent and has given so freely without any duress.
d. That individuals have received sufficient information on why their data is needed and how it will be used.

4. DATA USE

Personal information is of no value to any Massy company unless the business can make use of it. However, when personal information is accessed and shared which can be at the greatest risk of loss, corruption or theft, the company must ensure the following:

a. When working on personal data, employees should ensure that there is a protected screen installed on computers and computers are locked when left unattended.

b. Personal information should not be shared informally.

c. Data must be encrypted before being transferred or transmitted electronically.

d. Employees should not have saved copies of personal data stored on their computers, and or mobile devices.

e. Information passing between any Massy company's main office and sub- agencies must not go astray or be misdirected.

f. Third party entities to whom Massy has transferred data must agree to maintain the information confidentially, to maintain the security at the level maintained by Massy or higher and in accordance with the data protection laws of Barbados.

g. When accessing websites ensure that reasonable discretion is applied so as to not divulge any information to individuals unknowingly.

h. All security access levels for application must be password protected. (Please see the **Password Policy GITP-11** for creating strong passwords).

i. All employees should undergo Information Security Awareness Training, and their signatures should be on the training register, prior to be given access to personal information of customers and other users.

5. DATA STORAGE

Information and records relating to customers must be stored securely and must only be accessible to authorized staff. Information must only be stored for as long as it is needed or required by the law of the country. Sensitive information is to be physically stored on a server with restricted access to the area enforced, and all personally identifiable information must be stored encrypted.

6. ACCESS TO CUSTOMER INFORMATION

Any Massy company collecting and storing sensitive information on customers is required to follow IT best practice worldwide. This ensures that the IT infrastructure security is proactive and prevents unauthorized access to data. Each Massy company is to enforce authentication, segregation of duties, secure the services running on the server, set the right permissions on files and folders, secure the infrastructure using a firewall, perform regular audits and scans of the network for vulnerabilities and ensure that data is backed up regularly and stored at on offsite location. Any Massy company disclosing or transferring information to third party entities must also confirm and be reasonably satisfied that those third-party entities follow IT best practice worldwide before disclosing or transferring sensitive information.

7. DATA DISPOSAL

It is the responsibility of each Massy company to ensure that computers previously used by the organization that has been passed on or sold to the third party are properly disposed of. It is also the responsibility of each Massy company to ensure that all data and licensed software stored on the computer is non-recoverable. All company assets are to be disposed of in an eco-friendly manner. Company assets containing sensitive information should not be placed by the wayside to cause damage to the Massy image or reputation. Massy companies' assets should be disposed of through a recognized e-waste company bearing the Certificate of Environmental Clearance (CEC) seal.

8. VIOLATIONS

Any violations of the Data Protection Policy must be reported immediately to the ICT department of the respective Massy company and the employee's manager. Violating this policy or any of its tenets could result in disciplinary action.

9. ENFORCEMENT

The Massy Group will enforce the Security Policy Framework and establish standards, procedures, and protocols in support of the policy. Any employee found to have violated this policy may be subject to disciplinary action.

It is the responsibility of the Users to read, understand and comply with the various matters set out in this policy.

10. MODIFICATION TO THIS POLICY

Please note that from time to time this policy will be reviewed and changed to reflect IT standards and best practices, worldwide.

If you are in any doubt as to which laws, regulations, codes of conduct, and company guidance are relevant to your situation you should seek advice from your supervisor, HR representative, or legal department.

11. ACKNOWLEDGMENT OF DATA PROTECTION POLICY

This form is used to acknowledge receipt of and compliance with the company's Data Protection Policy.