DATA PROTECTION POLICY

Policy Owner	Data Protection Officer
Policy Approver(s)	Board of Directors
Related Policies	
Related Procedures	
Storage Location	Company Servers and Company approved Cloud applications
Effective Date	December 1, 2023
Next Review Date	December 1, 2027

TABLE OF CONTENTS

1. Background on the Data Protection Act 2020

Wisynco Group Limited ("**Wisynco**") is committed to processing data in accordance with its responsibilities under the Data Protection Act 2020. The Act was adopted by Jamaica's Parliament in 2020 and came into effect on December 1st, 2023 ("**the Act**"). It is designed to strengthen the control and personal autonomy of individuals over their personal data in line with current relevant international standards.

This Policy is designed to facilitate Wisynco's alignment with the Act as well as with international legal obligations.

2. Purpose

Wisynco recognizes that as part of our operations we must collect and process personal data. The purpose of this policy is to describe how personal data must be collected, handled and stored to meet Wisynco's data protection standards, comply with governing privacy and data protection laws, and respect individual rights. The purpose of this policy is as follows:

- Comply with the Data Protection Act and follow best practices.
- Protect the rights of employees, customers and any related data subjects as guaranteed by the Charter of Fundamental Rights and Freedoms.
- Ensure transparency around how Wisynco collects, stores and processes individuals' data.

3. Scope

This Data Protection Policy applies to all business processes, information systems and components, personnel, and physical areas of Wisynco. This policy applies to the collection, processing, storage, and handling of personal data related to any individual in both electronic and physical paper format.
Individuals or groups that this policy applies to include, but are not limited to:

- Executives and directors
- All employees, whether employed on a full-time or part-time basis, by Wisynco
- All previous employees, whether employed on a full-time or part-time basis, by Wisynco
- All job applicants of positions at Wisynco
- All contractors, suppliers and other people working on behalf of Wisynco
- All customers of Wisynco
- Any other data subject identified through the regular course of business by Wisynco

4. Policy and Procedures

4.1. Minimum Requirements:

- Employees will keep all data secure by taking sensible precautions and following guidelines outlined within this policy and any associated procedures.
- Data will not be shared informally; defined data access levels will be determined based on role and existing access controls.
- Wisynco will provide training to all employees to help them understand their responsibilities when handling data. Refer to the Security Awareness Training Policy for further details.
- Personal data will not be disclosed to any unauthorized person, either within the organization or externally without reasonable defined business requirement.

4.2. Data Collection:

- Wisynco and any affiliates will collect personal data in a manner that is fully transparent with data subjects and in accordance with the law.
- Users will refrain from collecting the personal data of any data subject without authorization from a direct manager or data protection officer.
- If personal data is collected from someone other than the data subject, the data subject will be informed of the collection unless one of the following criteria apply:
    - The data subject has received the required information by other means.
    - The information must remain confidential due to a professional secrecy obligation.
    - A national law expressly provides for the collection, processing, or transfer of the personal data.
- When determined that the notification of the data subject is required, notification should occur promptly and adhere to guidelines within the Consent Policy.
- When necessary, Wisynco will obtain consent from data subjects in accordance with the Consent Policy and through the authorization of the data protection officer.
- Consent from the data subject will be provided in writing.

- Wisynco's external-facing website(s) will include a privacy notice.

4.3. Data Storage:

- When data is stored electronically, it will be protected from unauthorized access, accidental deletion, and malicious hacking attempts.
- Wisynco will protect data with strong passwords. Refer to the Access Control Policy for further detail.
- Users will refrain from using removable media; if data is stored on removable media devices, they will be stored securely.
- Wisynco data will be stored on designated drives and servers and will only be uploaded to approved cloud computing service(s).
- Servers containing personal data will be sited in a secure location, away from general office space.
- Users will refrain from saving data directly to devices.
- Users will refrain from storing data on paper and only print when necessary.
- Paper documents or files should be kept in a locked drawer or filing cabinet unless they are actively being used.
- Wisynco users will ensure paper documents are not left where unauthorized persons could view them (e.g. on a printer).

4.4. Data Use

- Where applicable, Wisynco will provide each data subject with information regarding the processing of their information.
- Wisynco will consider the data subjects' perspective when processing personal data.
- All data processing must comply with the standards as set out in the Data Protection Act.
- When working with personal data, users will ensure screens are locked when left unattended.
- Wisynco users will not informally share personal data.
- Users will refer to their manager or to the data protection officer if personal data is anticipated to be transferred outside of the users' region.
- When possible, users will access personal data via a master copy or set of data.

4.5. Data Accuracy:

- Wisynco will take reasonable measures to ensure that personal data remains accurate.
- All users at Wisynco will take reasonable steps to ensure personal data is kept as accurate and up to date as possible.
- Data stored at Wisynco will be held in centralized locations. Users will not create unnecessary additional data sets.
- Where applicable, Wisynco will ensure data subjects can easily update their information.

4.6. Data Retention:

- Data should be regularly reviewed against the Records Retention Schedule. If no longer required, data should be deleted and disposed of. Refer to Records Retention Schedule for further detail.
- Paper documents will be shredded and disposed of securely when no longer required.

4.7. Data Protection:

- Security staff will use necessary physical and technical controls and organizational measures to ensure all infrastructure containing data is protected and secured. Refer to Access Control policy for further detail.
- Users will follow associated procedures and notify relevant staff when reporting incidents or data breaches. Refer to the Incident Response Policy for further detail.

4.8. Providing Information – Data Subject Requests:

- Wisynco will ensure that requests based on each of the following data subject rights can be satisfied:
    - Right of Access
    - Right to object to processing for the purpose of Direct Marketing
    - Objection to automated decision making and profiling
    - Right to Prevent Processing
    - Right to Data Portability
    - Data rectification
- Wisynco aims to ensure that individuals are aware that their data is being processed and they understand:

- How the data is being used
- How to exercise their rights

- Should Wisynco reasonably require further information in order to satisfy itself as to the identity of the data subject making the request, it shall inform the data subject of that requirement.
- Data subject rights requests will be managed by the data protection officer.
- Wisynco will respond to each data subject request within the time period set out in the Act for the specific request.
- When a data subject request cannot be adequately addressed, the following information will be provided to the data subject:
  - An acknowledgement of receipt of the request
  - Any information located to date
  - Details of any requested information or modifications that will not be provided to the data subject, the reason(s) for the refusal, and any procedures available for appealing the decision
  - An estimated date by which any remaining responses will be provided
  - An estimate of any costs to be paid by the data subject (e.g. where the payment of a prescribed fee under the Act is required in order for the request to be fulfilled)
  - The name and contact information of Wisynco point of contact

4.9. Use of Artificial Intelligence and Automated Processing:

Artificial intelligence, machine learning tools, automated decision-making tools, profiling tools, or similar technologies may only be used to process personal data where there is a clearly defined business purpose, an appropriate lawful basis for processing, and prior approval from the Data Protection Officer and Information and Technology Manager or their designates.

Personal data must not be entered into public or unapproved AI tools. Where AI tools are approved for use, users must only input the minimum personal data necessary for the approved purpose and must not upload sensitive personal data unless expressly approved by the Data Protection Officer following a documented risk assessment.

Where AI is used to support decisions about individuals, Wisynco will ensure that decisions are not based solely on automated processing where the decision produces legal, employment, financial, or similarly significant effects on the data subject, unless permitted by law and subject to appropriate safeguards, human review, and the data subject's rights under the Act.

Any procurement or use of third-party AI systems that process personal data must be subject to due diligence, contractual data protection terms, access controls, retention limits, confidentiality obligations, breach notification obligations, and restrictions on the vendor's further use of Wisynco data, including restrictions on using Wisynco data to train external AI models unless expressly approved.

4.10. Processing of Human Resources Data:

Human Resources data includes personal data relating to job applicants, employees, former employees, contractors, interns, directors, and other persons whose information is processed for workforce, recruitment, payroll, benefits, performance management, training, disciplinary, health and safety, security, legal, compliance, or related employment purposes.

HR data must be collected and processed only for specified, lawful, and necessary employment-related purposes. Access to HR data must be limited to authorized personnel with a legitimate business need, including Human Resources, Payroll, Legal, Compliance, Information and Technology, relevant managers, and approved service providers where required.

Sensitive HR data, including health information, biometric data, disciplinary records, investigation materials, background checks, medical certificates, disability-related information, and other sensitive personal data, must be handled with enhanced confidentiality, access restrictions, secure storage, and only where the processing is necessary and supported by an appropriate lawful basis.

Where HR data is processed using HR information systems, payroll systems, applicant tracking systems, attendance systems, CCTV/security systems, biometric systems, productivity tools, or AI-enabled tools, the relevant business owner must ensure that the use is transparent, proportionate, documented, and consistent with applicable privacy notices, employee communications, retention requirements, and approved access controls.

HR data must not be used for monitoring, profiling, disciplinary action, recruitment screening, performance assessment, redundancy selection, promotion decisions, or other employment decisions in a manner that is unfair, discriminatory, excessive, or inconsistent with the purpose for which the data was collected. Human review must be retained for material employment decisions.

HR data must be retained only for as long as required under the Records Retention Schedule, applicable law, contractual obligations, legitimate business requirements, or the establishment, exercise, or defence of legal claims. When HR data is no longer required, it must be securely deleted, anonymized, archived, or destroyed in accordance with applicable procedures.

4.11.Other Related Policies & Procedures

- Security Awareness Training Policy
- Data Retention Policy and Schedule
- Access Control Policy
- Data Subject Request Procedure
- Procedure for managing third party contracts
- Employee Privacy Notice
- Privacy Notice
- Consent Policy

4.12.Compliance

Each Wisynco person (employee and director) who handles personal data shall complete a Data Protection training exercise and on an annual basis, submit a self certification document in which indicates that the Wisynco person has read the policy, understands the contents therein and gives an undertaking to comply with the terms of the policy.

This certification exercise shall be managed by the Head of Department for each employee, where applicable and the Chairman of the Board for the directors where applicable.

4.13.Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at Wisynco. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

a. Disciplinary action according to applicable policies.
b. Termination of employment, subject to the relevant disciplinary procedures and policies as are applicable and the provisions of the Labour Code.
c. Legal action according to applicable laws and contractual agreements.

1. APPENDIX 1 - DEFINITIONS

Act: means the Data Protection Act, 2020 of Jamaica
Affiliate: means, with respect to any person, any other person directly or indirectly controlling, controlled by, or under common control with, such person, in each case from time to time
Data: Information in a format that can be processed, including electronic data and physical data.
Personal Data: Any information relating to an individual data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. This data could be anything from a name, an email address, geolocation data, or even a username or IP address.

Sensitive Personal Data: Any personal data that pertains to, or can be specifically attributed to an individual, that reveals information of the following sensitive nature: genetic or biometric data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, personal health information, information regarding the alleged commission of an offence.

Data Subject: An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Consent: Consent is any freely given, specific, informed, and unambiguous indication of a data subject's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

Company: means Wisynco and any Affiliates or subsidiaries

GDPR: means the General Data Protection Regulation.

Register of Systems: means a register of all systems or contexts in which personal data is processed by the Company.

Responsible person: see Section 3.0 Responsibilities And Accountability

Data Controller: The person; or public authority who, either alone or jointly in or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed, and where personal data are processed only for purposes which they are required under any enactment to be processed, the person on whom the obligation to process the personal data is imposed by or under that enactment is for the purposes of the Act a data controller. For the purposes of this policy, the Data Controller is either Wisynco, depending on which company is collecting and processing the personal data.

Data Processor: In relation to personal data, means any person other than an employee of the data controller, who processes the data on behalf of the data controller. This may include any independent contractors, outsourcing arrangements or otherwise which are processing personal data on behalf of the Company.

Processing Data: Any operation or set of operations that is performed upon personal data or sets of personal data, which includes obtaining, recording or storing the information or personal data, or carrying out any operation or set of operations (whether or not by automated means) on the information or data, including - (a) organisation, adaptation or alteration of the information or data; (b) retrieving, consulting or using the information or data; (c) disclosing the information or data by transmitting, disseminating or otherwise making it available; or (d) aligning, combining, blocking, erasing or destroying the information or data, or rendering the data anonymous.

Data Storage: These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data protection officer.

2. APPENDIX 2 - RESPONSIBILITIES AND ACCOUNTABILITY:

Personnel	Summary of Responsibility

Information and Technology Manager (or designate)	1. review and approve data protection policy at its inception 2. review policy at least annually. 3. oversee and improve cybersecurity awareness programs and risk management regularly. 4. collaborate with the .....team in leading the design, implementation, operation, and maintenance of the information security management system (ISMS) based on the ISO/ IEC 27000 series standards. 5. ensure periodic testing are conducted to evaluate the security posture of information security. 6. lead the design and operation of related compliance monitoring and improvement activities to ensure compliance both with internal security policies and applicable laws and regulations. 7. develop and manage controls to ensure compliance with the requirements of various security laws, standards, and regulations. 8. strictly comply with all relevant policies related to non-disclosure, non-competition, and the confidentiality of information. 9. constantly stay up to date on various web technologies and tools. 10. perform networking systems hardware and software upgrades and install security patches, as needed. 11. check and monitor the general health of networks and networking devices. 12. perform daily system monitoring, verify the integrity and availability of all hardware, server resources, systems, and IT processes, review system and application logs, and verify
Compliance Manager	1. lead the design and operation of related compliance monitoring and improvement activities to ensure compliance both with internal data privacy policies and applicable laws and regulations. 2. ensure that controls are implemented and operating effectively so that access to the personal data will not be shared with or provided to unauthorized parties. 3. ensure that controls are implemented and operating effectively so that additional documents and data are being stored appropriately and centralized to ensure the confidentiality, integrity, availability of the data .
Systems Administrators	Ensure that access to the personal data: 1. is restricted to authorized personnel only. 2. will not be shared with or provided to unauthorized parties. 3. appropriate back-up and disaster recovery solutions shall be in place. 4. when personal data is deleted this should be done safely, such that the data is irrecoverable.
Data Controller	Wisynco as Data controller shall: 1. register with the Information Commissioner's Office as an organisation that processes personal data. 2. ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. These purposes constitute employee data, payroll data, performance data and general communication with the organisation. 3. ensure that data is processed in the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests. 4. shall take reasonable steps to ensure personal data is accurate. 5. ensure that personal data is kept for no longer than necessary, the Company shall put in place an archiving policy for each area in which personal data is processed and review this process annually. 6. data should/must be retained, in accordance with archiving policy indicating for how long, and why. 7. ensure that personal data is stored securely using effective software that is kept-up-to-date. 8. ensure access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

Data Protection Officer	1. take responsibility for the data subject to ongoing compliance with this policy. 2. inform and advise the controller or processor and their employees of their obligations under data protection laws. 3. act as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights. 4. oversee and implement data protection strategies. 5. conduct regular assessments and audits to ensure compliance 6. in event of a breach, promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.
Employees	In the context of the work that an employee is doing on behalf of the Data Controller: 1. shall take reasonable steps to ensure personal data is accurate. 2. provide accurate information when reminded or asked to update their records. 3. access their personal data and any such requests made shall be dealt with in a timely manner.

3. APPENDIX 3 – GOVERNING LAWS REGULATIONS AND STANDARDS

Guidance	Clarification/Section
The Data Protection Act	Jamaican data privacy law
General Data Protection Regulation (GDPR) 2016/679	European Union (EU) data protection regulation

Document #	Title
	Data Protection Act 2020
	ISO/IEC 27000 Series Standards
ISO 9001: 2015	Clause 7. 5 Documented Information
	Charter of Fundamental Rights and Freedoms.

RATIFIED BY THE Board on April 30, 2026