Privacy & Data Protection Policy
(the "Policy")
Cyberati Group

1. PRIVACY & DATA PROTECTION

Credentia companies, M&S foundation, Cyberati entities and Unikclik entities are part of the Cyberati Group (hereinafter referred to as the "Group", "we", "us", endorsing and referring to this Privacy and Data Protection Policy recognise the importance of protecting the personal data of clients, employees, service providers and other relevant parties, as well as users of the Group's website/s, all collectively referred to as the "Parties". This Privacy & Data Protection Policy should be read in conjunction with any Data & Privacy policy and procedures as may have been individually adopted by each entity forming part of the Cyberati Group. We are registered as controller with the Data Protection Office in Mauritius.

To ensure compliance with the Data Protection Act 2017 of Mauritius, and any regulations that may come thereunder, and in respect of European union citizens, the law of the country of their residence for the purpose of the GDPR (the European Union General Data Protection Regulation, which came into force in 25 May 2018, the Group has implemented this data protection program, consisting of the following key components:

I. Written Policy and Procedures

We have implemented this Policy to protect personal data and privacy. The Policy provides the Parties with information regarding the purposes for processing their personal data, the lawful basis for processing, the retention period of their data and with whom the data will be shared. Business units, including the Information Technology (IT) and Operations departments, implement and maintain procedures to ensure the security and protection of personal data and manage other related privacy matters.

II. Appropriate Delegation of Authority

The Group has designated a Data Protection Officer (DPO) responsible for overseeing compliance related to data collection and processing by the Data Controller. The designated individual has relevant experience and the authority to oversee the implementation and maintenance of privacy standards across the Group.

III. Education and Awareness

All staff members, including new hires, undergo data protection training. The DPO, in coordination with designated staff, identifies employees subject to role-based privacy training requirements and facilitates mandatory training courses or seminars as necessary. The Group periodically provide refresher training to

employees handling client data. Training may include online courses, in-person lessons, or other instructive materials.

IV. Compliance Oversight

The DPO is tasked with evaluating new products, technologies, online activities, contracts, and regulations for potential privacy impacts and advising senior management on implementing corresponding privacy protections. Additionally, the DPO will maintain records to satisfy record-keeping obligations, and the Group will implement controls to recognize and respond to personal data breaches, including response plans and escalation procedures.

V. Periodic Assessments of Program Effectiveness

The Group will periodically evaluate and may adjust the program in light of risk assessment results, relevant findings by Compliance Officer and the DPO, or in response to significant changes in business practices, operations, or regulatory requirements.

2. CONTROL OF NON-PUBLIC INFORMATION

In the course of its business, the Group collects personal information about potential clients, employees, service providers, and other third parties. The Group is committed to maintaining the highest standards of integrity and aims to provide fair, secure, and appropriate methods for handling non-public personal information. All such activities are intended to be consistent with generally accepted privacy ethics and standard business practices.

To this end, the Group will adopt and implement adequate privacy policy measures. The principles of the Group's privacy policy include:

2.1 Personally Identifiable Information

The Group will collect personal information specifically and knowingly provided by clients, staff, service providers, and other third parties. Where applicable, the Group may use the personal information of clients to contact them regarding the Group's services or to provide feedback and updates related to their use of the services. The Group will only retain data necessary to offer its services and ensure continuity.

2.2 Privacy Statement Changes

The Group may modify its Privacy and Data Protection Policy at any time and as far as practicable, will notify clients of such changes to ensure they are aware of the conditions under which they provide personal information to the Group.

2.3 Retention of Records

The Group will retain personal information only as long as necessary and in compliance with applicable Mauritian laws regarding record-keeping, including for service provision or as required by law. Personal information no longer needed will be destroyed by shredding or other approved destruction methods to prevent unauthorized access unless regulatory requirements mandate its retention.

The Group will safeguard all client information in its custody and will develop and maintain security procedures to protect personal information against loss, theft, copying, unauthorized disclosure, use, or modification. Access to personal information is restricted to employees and authorised service providers with a legitimate need to know and use the information for their activities. The Group will not use clients' personal information for any other purpose unless authorised.

Your Consent
By accessing the Group's websites, you consent to the collection, maintenance, use, and disclosure of your personal data in accordance with this Privacy and Data Protection Policy.

Queries
If you have privacy-related questions not addressed by this Policy or any other concerns about how the Group uses your personal data, please contact us at: contact@cyberatidigital.com