OQATA WELLNESS SOLUTIONS

Naturally Inspired, Scientifically Proven.

Security Procedures for Personal and Payment Information

1. Purpose

The purpose of this document is to outline the security measures and procedures adopted by OQATA Wellness Solutions to safeguard the confidentiality, integrity, and availability of personal and financial information collected through our Online Store. As an organization committed to wellness, trust, and ethical business practices, we recognize that our customers entrust us with sensitive details when they shop online. Protecting this data is central to our operations, our brand reputation, and our compliance with industry regulations such as the Payment Card Industry Data Security Standard (PCI-DSS), General Data Protection Regulation (GDPR) principles, and local NITA-U ICT security guidelines.

2. Data Encryption

To ensure all information transmitted between customers and our online systems remains private and secure:

- We use Secure Socket Layer (SSL)/Transport Layer Security (TLS) encryption protocols across the entire Online Store, including checkout, customer accounts, and referral tracking pages.
- All personal data such as names, addresses, phone numbers, and login details are encrypted during transmission to prevent interception by unauthorized parties.
- Customers can verify security by checking for the padlock icon in their browser and ensuring the web address begins with https:// when accessing our store.
- Back-end systems, including our order management databases, also employ AES-256 encryption standards for data storage, which is considered a gold standard in security.

3. Secure Payment Processing

We do not directly process or store customer payment card details on our servers. Instead, we rely on trusted and established third-party payment processors that adhere to global financial security standards. These merchants handle all sensitive financial information on our behalf.

- Payments are securely processed through PESAPAL which is PCI-DSS certified.

- The payment gateways use tokenization technology, meaning that card numbers are replaced with randomly generated tokens, which cannot be reverse-engineered, thereby protecting financial details from exposure.
- These processors also employ fraud detection algorithms and real-time monitoring tools to identify unusual or suspicious transactions before they are completed.
- By outsourcing financial data handling to specialized providers, we minimize risks to our customers while maintaining compliance with global payment security frameworks.

4. Access Control and Authentication

Personal and payment-related data is only accessible to staff members whose roles require such access. To enforce this principle:

- Role-Based Access Control (RBAC): Staff are granted access to systems strictly according to their duties (e.g., Customer Service may view order status but not full payment details).
- Multi-Factor Authentication (MFA): Administrative accounts require at least two verification steps (such as password plus authentication app code) before access is granted.
- Regular Access Reviews: We periodically audit and update user privileges to ensure former employees or unauthorized persons cannot access sensitive data.
- Activity Logging: All system access attempts, whether successful or unsuccessful, are logged and reviewed to identify patterns of misuse or attempted breaches.

5. Data Storage and Retention

The way we handle customer data after it is collected is equally important:

- Customer information is stored in secure databases that are protected by firewalls and encryption technology.
- Payment card details are never stored on OQATA servers. Instead, secure transaction tokens provided by our payment processors are stored for reference in recurring transactions or refunds.
- Personal data is only retained for as long as it is necessary to fulfill orders, meet legal and tax requirements, or resolve disputes. After this period, the data is securely destroyed or anonymized.
- Regular backups of customer data are performed and encrypted, ensuring recovery is possible in the event of system failure or disaster.

6. Network and System Security

OQATA Wellness Solutions invests in modern security infrastructure to protect all systems connected to its online store:

- Firewalls: Multiple layers of firewalls separate the online store environment from unauthorized networks.
- Intrusion Detection and Prevention Systems (IDPS): Our systems continuously monitor for suspicious activity, unusual logins, or potential attacks.
- Malware Protection: Enterprise-grade anti-malware and anti-virus solutions are deployed across servers and endpoints to prevent infections.
- Security Patching: All software, plugins, and operating systems are regularly updated with security patches to minimize vulnerabilities.
- Segregation of Systems: Payment systems, customer databases, and public-facing services are separated into different environments to reduce exposure in case of breach.

7. Monitoring and Auditing

OQATA Wellness Solutions maintains a proactive stance toward risk detection:

- Continuous monitoring of online store activities ensures that any unauthorized attempt to access sensitive data is flagged in real-time.
- Automated alerts are triggered for irregular transactions, failed logins, or unexpected changes in system files.
- Routine internal audits and third-party penetration testing are conducted to identify and patch potential weaknesses.
- Compliance reviews are carried out to verify that we consistently align with PCI-DSS, NITA-U, and international data security best practices.

8. Incident Response and Breach Management

While we maintain strong defenses, we also prepare for unexpected incidents:

- A documented Incident Response Plan exists to manage security breaches quickly and effectively.
- In the event of a suspected or confirmed data breach, the following steps are taken:
    - Immediate isolation of affected systems.
    - Investigation and identification of root causes.
    - Containment and mitigation to prevent further data loss.

- Notification of impacted customers and relevant regulators in line with legal requirements.
- Remediation steps, including patching vulnerabilities and updating defenses.

9. Customer Responsibilities

We also encourage our customers to take precautions in safeguarding their accounts:

- Customers should use unique and strong passwords, combining letters, numbers, and symbols.
- Login details must be kept confidential and not shared with others.
- Customers are advised to access our store only via trusted devices and secure internet connections.
- Suspicious activities, such as unknown logins or unrecognized charges, should be reported immediately to OQATA Wellness Solutions Support.

10. Continuous Improvement and Compliance

Cybersecurity threats evolve rapidly, and our procedures are continuously reviewed to remain relevant:

- We benchmark our security framework against global standards, including ISO/IEC 27001 Information Security Management Systems.
- Updates to policies, systems, and tools are made in response to new threats, regulatory changes, or customer needs.
- OQATA Wellness Solutions is committed to transparency, ensuring that customers are kept informed of how their data is used, stored, and protected.