Information technology and data security policy

Sphere Commodities Group Pte Ltd and its affiliated companies ("Sphere Group") is committed to safeguarding sensitive information, maintaining the integrity of our IT systems, and ensuring compliance with applicable data protection laws in Australia, Singapore, and the Philippines. As a company operating in the electronic waste recycling industry, we recognize the critical importance of protecting data stored on devices we handle and maintaining robust IT and data security practices.

1. Purpose

This policy outlines our commitment to:

- Protecting company, customer, and partner information from unauthorized access, disclosure, alteration, or destruction.
- Establishing secure handling practices for data-bearing electronic devices.
- Ensuring compliance with data protection and cybersecurity regulations in the regions we operate.

2. Scope

This policy applies to all employees, contractors, third-party service providers, and partners involved in handling IT systems, sensitive data, or data-bearing devices in our operations in Australia, Singapore, and the Philippines.

3. Applicable Laws & Regulations

This policy aligns with:

Australia: Privacy Act 1988 and the Notifiable Data Breaches (NDB) scheme.

Singapore: Personal Data Protection Act (PDPA).

Philippines: Data Privacy Act of 2012 (RA 10173).

4. Responsibilities

Management Responsibilities

- Establish and maintain IT security policies and procedures.
- Conduct regular risk assessments to identify and address potential vulnerabilities.
- Ensure compliance with applicable laws and regulations.

Employee Responsibilities

- Adhere to this policy and any related procedures.
- Report suspected data breaches, phishing attempts, or other security incidents immediately.
- Use company IT resources responsibly and securely.

5. Data Security for Electronic Waste Recycling

Secure Handling of Data-Bearing Devices

Data-bearing devices (e.g., hard drives, SSDs, and mobile phones) received for recycling will be securely stored and tracked.

Data on devices will be irreversibly destroyed using industry-standard methods (e.g., degaussing, shredding, or certified data wiping).

Certificates of data destruction will be issued to customers upon request.

Chain of Custody

Maintain a documented chain of custody for all data-bearing devices to prevent unauthorized access or loss during transport and processing.

6. IT Systems and Infrastructure Security policy

Access Control

Restrict access to sensitive information and systems to authorized personnel only.

Use multi-factor authentication (MFA) and strong passwords for all critical systems.

Review and update access rights regularly.

Data Encryption

Encrypt sensitive data at rest and in transit to prevent unauthorized access.

Ensure encryption methods meet industry standards.

Network Security

Deploy firewalls, intrusion detection systems, and antivirus software to protect IT networks.

Regularly update software and systems to mitigate vulnerabilities.

Remote Work Security

Provide secure remote access through virtual private networks (VPNs).

Require remote workers to use company-approved devices with up-to-date security patches.

7. Data Privacy and Protection

Collect and process personal data in accordance with applicable data protection laws.

Limit data collection to what is necessary for business purposes and ensure its proper disposal when no longer needed.

Provide training to employees on data privacy laws and best practices.

8. Incident Response and Reporting

Incident Response Plan

Develop and maintain an incident response plan to address cybersecurity and data breaches.

Respond promptly to incidents to minimize damage and recover operations.

Reporting Obligations

Notify affected individuals and relevant authorities in compliance with the NDB scheme (Australia), PDPA (Singapore), and Data Privacy Act (Philippines) in the event of a data breach.

Maintain detailed records of incidents, investigations, and remediation actions.

9. Monitoring and Audits

Conduct regular audits of IT systems and processes to identify and address security risks.

Monitor systems for unusual activity or potential breaches using advanced monitoring tools.

Review this policy annually to ensure its effectiveness and alignment with regulatory requirements.

10. Training and Awareness

Provide mandatory IT and data security training for all employees and contractors.

Educate staff on identifying phishing, social engineering, and other cybersecurity threats.

Reinforce the importance of secure handling of data-bearing devices and compliance with legal obligations.

11. Consequences of Non-Compliance

Violations of this policy may result in disciplinary action, including termination of employment or contracts. Serious breaches may be reported to the relevant authorities for further action.

12. Review and Updates

This policy will be reviewed annually or as required by changes in legislation, technology, or business operations to ensure its continued relevance and effectiveness.

13. Contact Information

For questions, guidance, or to report concerns about IT and data security, please contact:

- Australia: Douglas Hunt, Douglas.Hunt@spheregroup.global PH: +61 439 876 116
- Singapore: Michael Abundo, Michael.Abundo@spheregroup.global PH: +65 9066 3584
- Philippines: Weslie Capute, Weslie.Capute@spheregroup.global PH: +63 977 821 1716

By adhering to this Information Technology and Data Security Policy, the Sphere Group demonstrates its commitment to protecting sensitive information, maintaining IT system integrity, and upholding the trust of customers and stakeholders in the electronic waste recycling industry.

Approved by the Board

January 2026