FEBRUARY 24, 2020

CX STUDIO

INFORMATION SECURITY POLICY

AGRICULTURAL COMPANY

QUEENSTAR MANTE-BONSRA
CV LIMITED
GHANA

	Document Title: Information Security Policy	Author: IT Security Officer
	DOCUMENT ID: C.V.L/INF/CV002	Classification: Internal Use Only
	Version: 2.0	Date: 24-Feb-2020

	Prepared by	Reviewed and Authorised By
Name:		
Job Title		
Signature		
Date		

Table of Contents

1.Introduction ... 2

1.1 Purpose ... 2

2. Scope and Applicability ... 3

3. Key Definitions ... 3

4. Governance and Responsibilities ... 3

5. Security Framework and Controls ... 4

5.1 Physical Security Controls ... 4

5.2 Cybersecurity Controls ... 4

5.3 Operational Security Controls ... 4

5.4 Environmental and Health Safety Controls ... 5

6. Compliance and Legal Obligations ... 5

7. Incident Management and Response ... 5

8. Enforcement and Violations ... 6

9. Policy Review and Continuous Improvement ... 6

10. Security Awareness and Training ... 6

11. References ... 7

1. Introduction

C.V.Limited is a leader in sustainable farming and food security in Ghana, dedicated to producing premium agricultural products through responsible and innovative practices. With operations ranging from crop production to supply chain management and distribution, C.V. Limited serve both local and international markets, ensuring the highest standards of quality and efficiency in everything C.V.Limited do.

At the core of our mission is a commitment to sustainability and community development. C.V.Limited prioritize environmentally responsible farming methods, the welfare of our employees, and strict adherence to local and global regulations. The company's approach integrates modern agricultural technologies with traditional farming knowledge, allowing us to increase productivity while conserving natural resources.

Through strategic partnerships, continuous innovation, and a deep-rooted connection to the communities C.V.Limited serve, the company's aim to make a positive and lasting impact on Ghana's agricultural landscape. As C.V.Limited grow, the company remain committed to improving livelihoods, fostering economic development, and contributing to a more resilient food system for future generations**.**

1.1 Purpose

The purpose of this security policy is to safeguard the agriculture company's physical and digital assets, protect employees, ensure business continuity, and maintain compliance with local and international regulations. The policy seeks to mitigate risks related to physical threats, cyber threats, environmental hazards, and operational disruptions, ensuring the company can continue its operations effectively.

2. Scope and Applicability

This policy applies to all personnel, including employees, contractors, consultants, vendors, and third-party partners. It covers all assets, including physical facilities, digital infrastructure, agricultural production areas, data systems, and supply chain processes.

3. Key Definitions

- **Sensitive Information:** Data that must be protected from unauthorized access, including personal data, financial records, and intellectual property.
- **Physical Security:** Measures to protect physical locations (e.g., farms, warehouses, offices) from threats such as theft, trespassing, and environmental hazards.
- **Cybersecurity:** Actions taken to protect IT systems and networks from digital threats like hacking, malware, and data breaches.
- **Business Continuity:** Processes and systems designed to ensure the company can continue operating in the event of a disruption.

4. Governance and Responsibilities

- **Board of Directors:** Oversees security governance and ensures alignment with company objectives.
- **Chief Security Officer (CSO):** Responsible for implementing the security policy and coordinating physical and digital security measures.
- **IT Security Team:** Manages cybersecurity efforts, including monitoring networks, responding to incidents, and implementing preventive measures.
- **Physical Security Team:** Manages the physical security of farms, warehouses, and production facilities, including access control and surveillance.
- **Compliance Officer:** Ensures the company adheres to legal and regulatory requirements, including data protection and environmental standards.
- **All Employees:** Are required to comply with this policy, report suspicious activity, and participate in security awareness programs.

5. Security Framework and Controls

5.1 Physical Security Controls

- Use physical barriers such as fences, locked gates, and security checkpoints to prevent unauthorized entry. Sensitive areas (e.g., pesticide storage) require biometric or keycard access.
- Install security cameras in high-risk areas, including warehouse entry points and farm perimeters. Monitor and regularly review footage.
- Install fire suppression systems and flood prevention mechanisms in key facilities. Emergency evacuation plans must be in place for all sites.

5.2 Cybersecurity Controls

- Implement firewalls, intrusion detection systems, and VPNs to protect internal networks from unauthorized access. Ensure all external connections are secure.
- Ensure that sensitive data is encrypted at rest and during transmission. Limit access to data based on job roles.
- Develop a procedure for responding to cyber incidents, including data breaches and malware attacks. The plan should outline roles, responsibilities, and response timelines.
- Conduct regular cybersecurity training, focusing on recognizing phishing attempts, proper password management, and secure handling of company data.

5.3 Operational Security Controls

- Assess third-party vendors for compliance with the company’s security standards. Implement contractual clauses that mandate adherence to cybersecurity and physical security protocols.
- Maintain a current inventory of all assets (both digital and physical), and classify them based on their criticality to business operations.

- Regularly update and test business continuity and disaster recovery plans to ensure the company can quickly recover from disruptions, including cyberattacks or natural disasters.

5.4 Environmental and Health Safety Controls

- Ensure compliance with Ghana's environmental protection regulations. Monitor the use of pesticides, water consumption, and soil health to prevent environmental degradation.
- Implement occupational health and safety procedures that address risks unique to agriculture (e.g., machinery safety, handling of hazardous chemicals). Conduct regular safety drills and audits.
- Ensure farming practices comply with global agricultural sustainability standards to promote long-term environmental health and food safety.

6. Compliance and Legal Obligations

- Ensure compliance with the Ghana Data Protection Act (2012 Act 843) and other relevant local laws related to environmental and health safety.
- Adhere to ISO 27001 (Information Security), ISO 22301 (Business Continuity), and ISO 14001 (Environmental Management) standards. Ensure continuous compliance with GDPR if handling EU customer data.
- Conduct annual audits to assess compliance with internal policies and external legal obligations. Use the results to improve security controls.

7. Incident Management and Response

- All employees must immediately report security incidents (e.g., physical breaches, cyberattacks) to the CSO or designated incident response team. A clear reporting chain will be established for escalating incidents.
- Each incident should follow the "identify, contain, eradicate, and recover" approach. Lessons learned from each incident should be documented and used to update procedures.

- Conduct a post-mortem after any significant incident to determine root causes, improve response strategies, and prevent recurrence.

8. Enforcement and Violations

- Non-compliance with this policy will result in disciplinary action, ranging from warnings to termination, depending on the severity of the violation.
- Employees are encouraged to report policy violations anonymously. Any retaliatory action against whistleblowers will not be tolerated.
- Violations of a critical nature will be escalated to the Board of Directors and legal teams for investigation.

9. Policy Review and Continuous Improvement

- This policy will be reviewed annually by the Chief Security Officer in collaboration with other key stakeholders. Updates will be based on changes in the business environment, regulatory requirements, and emerging security threats.
- Findings from internal audits, external assessments, and incident responses will be used to continuously enhance the policy.

10. Security Awareness and Training

- All employees must participate in annual security awareness training, with additional specialized training for key roles such as IT staff, farm managers, and warehouse personnel.
- Regular simulations (e.g., phishing tests) will be conducted to assess employee awareness and readiness. Results will inform targeted training efforts.
- Security updates, best practices, and guidelines will be regularly shared with employees through internal channels such as newsletters and the intranet.

11. References

- ISO/IEC 27001:2013 Information Security Management Systems (ISMS)
- ISO 22301:2019 Business Continuity Management Systems
- ISO 45001:2018 Occupational Health and Safety Management Systems
- ISO 14001:2015 Environmental Management Systems
- Ghana Data Protection Act, 2012 (Act 843)
- Global GAP (Good Agricultural Practices)
- National Institute of Standards and Technology (NIST) SP 800-53