CHAMELEON

FOR OUR SMARTER WORLD

By Theodore Savvidis and Nathan Tien Le Nguyen

Chameleon Security Information Policy

1. Introduction

This Security Information Policy outlines Chameleon's commitment to protecting the confidentiality, integrity, and availability of its information assets. This policy applies to all employees, contractors, and third-party vendors who access or handle Chameleon's data.

2. Data Security

- **Data Classification:** Chameleon will classify its data based on sensitivity (e.g., public, confidential, highly confidential). This classification will determine the appropriate security controls for each data type.
- **Data Access:** Access to Chameleon's data will be granted on a least privilege basis. Users will only be granted access to the information they need to perform their job duties.
- **Data Encryption:** All data at rest will be encrypted using industry-standard algorithms like AES-256. Data in transit will be secured using strong TLS encryption protocols.

3. User Authentication and Access Control

- **Strong Passwords:** Chameleon will enforce strong password policies for all user accounts. This includes minimum password length, complexity requirements, and regular password rotation.
- **Multi-Factor Authentication (MFA):** MFA will be required for access to all sensitive systems and applications. This adds an extra layer of security beyond just a username and password.
- **User Activity Monitoring:** User activity on critical systems will be monitored to detect suspicious activity.

4. System and Network Security

- **Vulnerability Management:** Chameleon will conduct regular vulnerability scans of its systems and applications. Identified vulnerabilities will be prioritized and addressed promptly.
- **Firewalls:** Firewalls will be deployed to control network traffic and prevent unauthorized access.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** IDS/IPS systems will be implemented to detect and prevent malicious network activity.
- **Secure Coding Practices:** Secure coding practices will be encouraged to minimize the risk of software vulnerabilities.

5. Incident Response

- Chameleon will establish a process for identifying, reporting, and responding to security incidents. This process will include procedures for data breach notification, containment, eradication, and recovery.

- All employees will be trained on the incident response process and their role in reporting suspicious activity.

6. Third-Party Vendors

- Chameleon will conduct due diligence on all third-party vendors before granting them access to its data.
- Contracts with third-party vendors will include clauses requiring them to maintain appropriate security controls to protect Chameleon's data.

7. Security Awareness and Training

- Chameleon will provide regular security awareness training to all employees to educate them on cybersecurity best practices and how to protect company data.
- Training will cover topics such as password security, phishing attacks, social engineering, and data security procedures.

8. Policy Review and Updates

- This Policy will be reviewed and updated periodically to reflect changes in technology, threats, and regulations.

9. Compliance

Chameleon will comply with all applicable data security laws and regulations, such as GDPR and CCPA.

10. Contact

For any questions or concerns regarding this Security Information Policy, please contact the Security Team.