CHAMELEON

FOR OUR SMARTER WORLD

IoT Policy Document

17 March 2024

Contents

Introduction

Chameleon recognises the significance of the Internet of Things (IoT) in today's technological landscape. The IoT represents an ecosystem of web-enabled smart devices, including phones, suburban traffic systems, and domestic appliances. These devices utilise embedded systems such as processors, sensors, and communication hardware to collect, send, and act on data acquired from their environments. These solutions aim to enhance various aspects of life through the application of smart city technologies, including the development of smarter cities, homes, transportation, and energy management systems.

Scope & Purpose

This policy document outlines Chameleon's approach to utilising IoT technologies responsibly and securely in alignment with our goals of researching, creating, testing, documenting, and deploying IoT-based solutions. The scope of this IoT policy defines the guidelines and rules governing the deployment, management, and usage of IoT devices and systems within the organisation, encompassing all employees, contractors, and any individuals with access to company information assets. For the purposes of this document IoT refers to the collective network of internet connected devices and the technology that facilitates communication between these devices.

Roles and Responsibilities:

The Chief Information Officer (CIO) is responsible for overseeing all IoT initiatives and ensuring alignment with organisational objectives. The Chameleon Security team is responsible for testing and implementing security measures to protect IoT devices and data.

Data Handling and Privacy:

To ensure the responsible handling of IoT data, the following guidelines are established:

- IoT data collected from sensors and devices must be stored securely. Access controls should restrict IoT data to individuals with a legitimate need-to-know basis through authorisation requirements.
- Users must provide consent before any personally identifiable information is collected through IoT devices. Transparent privacy notices should detail the types of data collected, its intended use, and any third parties with whom it may be shared.
- Anonymisation or pseudonymisation techniques should be employed before storing or processing IoT data to safeguard individual privacy.
- Regular audits and assessments of data handling practices should be conducted to ensure ongoing compliance with data protection regulations and industry standards.

Security Risk Management

Security strategies should be implemented to minimise potential risks including:

- Implementing robust security measures to protect IoT devices, networks, and data from unauthorised access, breaches, and cyber threats.
- Intrusion detection systems (IDS): Implementing IDS to monitor network traffic for suspicious activities and detect potential security breaches in real-time.
- Regularly updating firmware and software patches to address security vulnerabilities and mitigate risks associated with IoT deployments.
- Conducting periodic risk assessments and audits to identify and address potential security gaps in IoT systems and infrastructure.

Compliance and Governance

Chameleon is committed to upholding transparency, and accountability in its IoT initiatives. To ensure compliance with relevant laws, regulations, and industry standards, the company will:

- Establish a governance structure to oversee IoT activities and ensure alignment with organisational goals and values.
- Conduct regular reviews and audits of IoT policies, procedures, and practices to identify areas for improvement and address compliance issues.
- Provide ongoing training and awareness programs for employees involved in IoT projects to promote a culture of compliance and ethical behaviour.

Chameleon IoT policies for collecting, storing, and processing data generated by IoT devices must comply with relevant international data protection regulations including the GDPR and the CCPA.

Documentation and Review:

IoT deployments must be documented. Documentation should include details of IoT devices including tracking serial numbers, location, and usage such as data flows and security controls for deployed IoT devices.

Regular assessments should be conducted to ensure adherence to policies and identify areas for improvement. Personnel training should be regularly undertaken to provide updates on IoT security risks, best practices, and individual responsibilities when using or managing IoT devices.

Conclusion

Chameleon recognises the transformative potential of IoT technologies in improving the quality of life and driving sustainable development. By adhering to the principles outlined in this policy document and working collaboratively with stakeholders, Chameleon aims to harness the power of IoT responsibly and ethically to create positive impact for individuals, communities, and society as a whole.