Chameleon Website
Digital Preservation Policy

CHAMELEON

FOR OUR SMARTER WORLD

LEON NETTO

1. Introduction

The Chameleon organisation is aware of the importance of preserving digital assets hosted on the Google Cloud Platform (GCP), including the Chameleon web application which is a containerised application, code repositories, and databases.

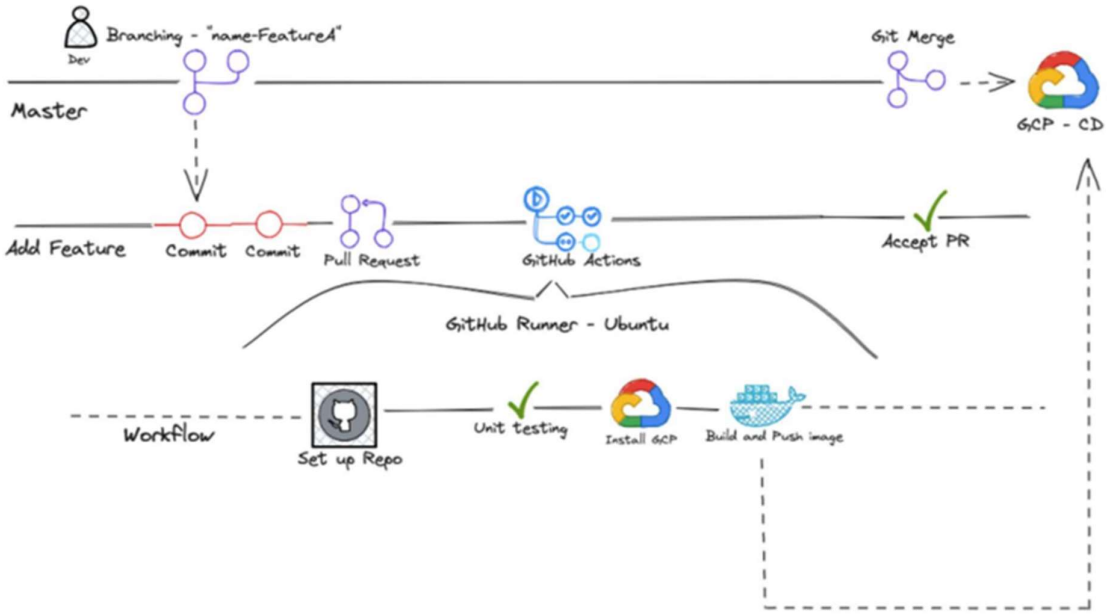
This Digital Preservation Policy establishes guidelines and procedures for the management and preservation of digital resources within this infrastructure.

2. Scope

This policy has been created in line with the CI/CD Pipeline and Deployment documentation developed by Mukund Srinivasan (previous team member of the Chameleon Website team). The policy applies to all digital assets hosted on the Google Cloud Platform within the Chameleon website infrastructure, including but not limited to:

- Docker container images stored in the Google Cloud Container Registry.
- Source code repositories hosted on GitHub.
- GitHub Actions workflows for code changes to deployment.
- MySQL databases used to store user login details for applications.

CI/CD Pipeline



Reference: CI/CD Pipeline and Deployment documentation

3. Purpose

The purpose of this policy is to ensure the integrity, availability, and longevity of digital resources for the Chameleon website. It aims to address:

- Long-term accessibility, integrity, and security of digital assets hosted on the Google Cloud Platform.
- Legal and regulatory requirements related to data protection, intellectual property rights, and digital preservation.
- Risk mitigation associated with data loss, unauthorised access, and technological obsolescence.
- Efficient management, detection, and retrieval of digital items through standardised metadata and access controls.

4. Preservation Strategies

The preservation activities within the Google Cloud Platform environment shall be guided by the following digital preservation strategies:

- **Security**: Robust security measures to protect digital assets from unauthorised access, data breaches, and cyber threats must be implemented.
- **Versioning**: Maintain version control for code repositories and container images to track changes and facilitate rollback procedures if necessary.
- **Backup**: Implement backup mechanisms for important digital assets to prevent data loss due to data corruption or service disruptions and ensure business continuity.
- **Compliance**: Adhere to relevant data protection regulations which include ISO and NIST guidelines and other industry standards for digital preservation.
- **Documentation**: Document all aspects of digital assets, including metadata, configuration settings, and deployment procedures, should resources and processes need to be reproduced and for individual accountability.

5. Task and Responsibilities

The responsibilities of the digital preservation tasks for the Chameleon Website are shared amongst the Chameleon Website team and the Chameleon Security Team.

The Chameleon Website team are responsible for the following tasks within the GCP environment:

- Managing the technical infrastructure, access controls, and security settings within the GCP environment.

- Maintaining version control, CI/CD pipelines, and Docker container images in compliance with this policy and industry guidelines.
- Managing databases, including backup, replication, and encryption of user login details in accordance with data protection regulations.

The Chameleon Security team are responsible for:

- Updating the policy in line with current security controls and guidelines.
- Conducting annual risk assessments to ensure digital preservation activities are being carried out.

6. Implementation

The implementation of this policy for the services within the Google Cloud Platform environment must include the following steps:

- Configuration of access controls and security settings to restrict access to digital resources based on roles and permissions.
- Docker images should be version controlled for rollback capabilities and tracking changes and Git must be used to manage source code changes.
- Implementation of automated backup and disaster recovery procedures for Docker container images, GitHub repository, GitHub Actions and databases.
- Encrypt data stored in the database with the most current and effective security industry standards to protect the confidentiality of Chameleon users.
- Integration of monitoring and alerting systems to detect and respond to security incidents, data breaches, or service disruptions.
- Implement ongoing testing to ensure the reliability of digital resources and develop and test a comprehensive Disaster Recovery Plan.
- Regular audits and reviews of digital preservation practices to assess compliance with this policy and identify areas for improvement.

7. Review

This policy shall be reviewed annually by the Chameleon Security team in collaboration with the Chameleon Website team to reflect changes in technology, regulations, or organisational requirements.