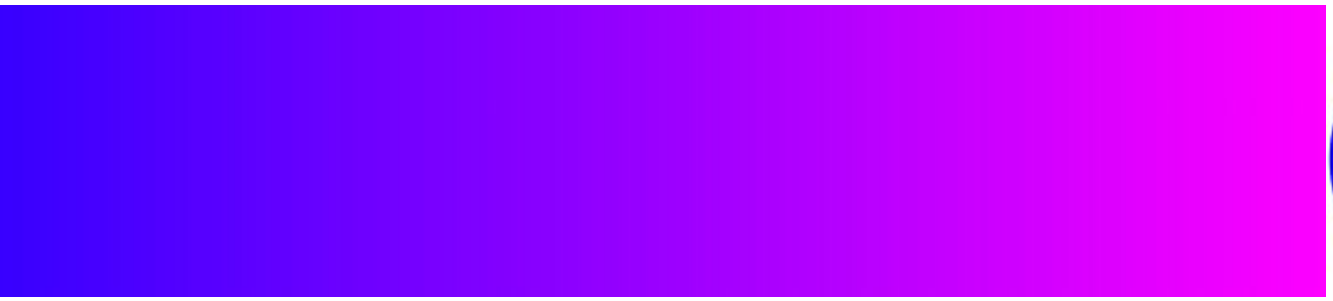
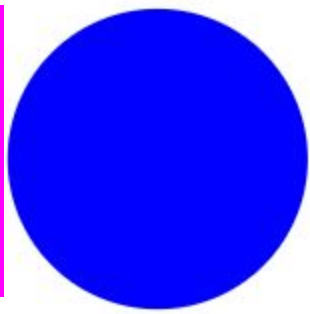
CIRCLES.LIFE

Security Whitepaper

As at Dec 2020





INTRODUCTION

Circles.Life is more than just Asia's first fully digital telco. Since we launched in 2016, we remained focused on our mission to give power back to the consumer. Through our game-changing digital products and no-contract, data-focused mobile plans, we're revolutionizing the digital services industry through a customer-centric user journey.

At Circles, we know that the **Confidentiality**, **Integrity**, and **Availability** of information is of paramount importance for everything we do. Hence, we believe that data security is the responsibility of the entire organisation.

In this document, we seek to explain our approach to security and be transparent on our security practices.

GOVERNANCE. 2

OPERATIONAL SECURITY. 2

APPLICATION SECURITY. 3

DATA SECURITY. 3

PHYSICAL SECURITY. 3

*"At **Circles**, we know that the **Confidentiality**, **Integrity**, and **Availability** is of **Paramount Importance** for everything we do."*

GOVERNANCE

INFORMATION SECURITY

Information Security falls under the purview of Circles Information Security Office, led by the Global Chief Information Security Officer (CISO). The office consists of three pillars namely - Cyber Operations, Cyber Governance and Cyber Defence which drives a variety of security initiatives and supports the implementation of security best practices.

POLICIES & TRAINING

All Circles' employees are required to understand, follow and agree to internal policies/standards as part of the onboarding process. Security training is mandated for all employees and covers a wide range of topics such as acceptable use, security testing, incident reporting and data privacy.

OPERATIONAL SECURITY

ENDPOINT & SERVER PROTECTION

Workstations issued to Circles employees are configured and updated with the latest OS version.

In ensuring compliance to Circles' policies and procedures, we have implemented Endpoint and Patch Management solutions so that employees' workstations are always protected and stay up to date.

Servers that are provisioned for critical and customer-centric activities are hardened in accordance to security best practices.

SECURITY OPERATION CENTER (SOC)

We have a dedicated team of analysts that actively monitor and assess any potential cyber security incident(s). The team follows a set of processes when any incident(s) occurs.

Incident(s) are prioritised in accordance to its severity - for example, those impacting our customers are assigned the highest priority. The team tracks and closes the incident(s) with appropriate corrective actions.

Where applicable, we will implement controls to prevent recurrence of similar incident(s).

VULNERABILITY MANAGEMENT

Circles has a robust vulnerability management program that continuously scans for security threats using a combination of commercially available tools, automated and manual penetration testing efforts, assurance reviews and 24x7 active monitoring by our SOC.

IDENTITY & ACCESS MANAGEMENT

Circles implement and enforce Single Sign-on (SSO) on our systems and applications. SSO simplifies the login process for our employees while ensuring an effective centralized compliance and access control management.

Furthermore, we adhere to the principles of least privileges access and role-based permissions to minimize the risk of a data leakage. Access to customers' information is strictly granted to employees on a need-to-know, need-to-do basis.

THIRD-PARTY MANAGEMENT

Circles engages on a number of third-party vendors to provide specific services. Prior to onboarding, we conduct due diligence on them to evaluate that they provide a certain level of security and privacy based on the scope of services rendered.

APPLICATION SECURITY

APPLICATION ARCHITECTURE

Circles systems (websites, mobile applications and backends) are tiered in logical segmentation that separate presentation from business logic and underlying data storage.

SECURE DEVELOPMENT

In Circles, we believe in security by design. All functionalities are planned with security in mind to protect our product(s) against security threats and data privacy abuses.

Circles follows best practices throughout our software development process. Source code is stored in version control repository with controlled accesses. Code changes are subject to continuous integration testing to identify potential security issues and resolve them.

SECURITY TESTING & VULNERABILITY DISCLOSURE PROGRAM

Circles has a dedicated team to perform periodical penetration testing to verify our resilience against cyber attacks.

Our security testing methodology integrate and makes active reference to industry led standards such as Open Web Application Security Project (OWASP) and Common Weakness Enumeration (CWE). Findings from the testing(s) performed are categorised by their severity and tracked till resolution.

Circles launched its public vulnerability disclosure program with HackerOne in December 2020. Please refer to the link[2] for more information on the program.

DATA SECURITY

DATA PRIVACY

Circles respect the privacy of our customers' data and we adhere to the data privacy regulations of respective countries that we operate in. Please refer to the respective link[1] for more details on our privacy policy.

DATA AT REST

Circles uses industry standard encryption algorithm(s) to encrypt sensitive information including customer data at rest on the database(s). The encryption key(s) are stored in secure infrastructure and separate server with limited access to only appropriate personnel.

DATA IN TRANSIT

Circles uses SSL/TLS encryption during data transfer to protect data in transit between our applications and servers. As such, a secure tunnel is created during data transfer keeping end to end communication secure.

1. *https://circles-legal.s3-ap-southeast-1.amazonaws.com/au/circles.life-privacy-policy.pdf*
2. *https://www.circles.life/au/vulnerability-disclosure-program/*

PHYSICAL SECURITY

@CIRCLES

Circles leverages Amazon Web Services (AWS) and Google Cloud Platform (GCP) for our systems including website(s) and mobile application(s).

AWS and GCP offer state of the art physical protection for all the underlying infrastructure that supports our platform. The infrastructure security of these providers complies with security best practices and a variety of IT security standards including ISO 27001 and attested via respective SOC 1/2/3 reports.

For more details on the security controls, please refer to the following links:

AWS
https://aws.amazon.com/security

GCP
https://cloud.google.com/security

CONCLUSION

Circles treats information security practices as a competitive advantage; our customers and stakeholders can be rest assured that securing data is part of an integral part of our business. We will continue to work hard to maintain your trust and by staying a step ahead to retain the same as our value proposition.

If you have any further questions, please don't hesitate to contact our security team at *infosec@circles.asia*.