

60/2018 -1




Exp: 06/26/2019

Process Owner: IT Operations	FORM	F-ITO-SEC-1.1
	Security Exception Request	

Items I, II, III, IV, V, VI to be accomplished by the IT Operations
 Items VII, VIII, IX to be accomplished by Requesting Business Unit

I. Request Information		
Requesting Business Unit	Circles Life	
Requestor	Sherryl Tabat	
Date Requested	June 26, 2018	Time: 12:35pm
Date Required	June 26, 2018	
Receiving IT Operations Personnel	Marlon De Guzman	

II. Detailed Request Information
<p>Request: Access(wifi) for WhatsApp application in mobile phone of Circles Life support team (Analie Barairo, Sherryl Tabat, Brianne Salazar and Amiel Cua)</p> <p>Proposed validity of request: June 26, 2018 – June 26, 2019</p> <p>Location: 8th Floor</p> <p>Mobile Details:</p> <p>Brand: Samsung Model: Galaxy J5 Serial no: RV1G71RZMWR MAC address: 50:F0:D3:9E:C0:BD</p> <p>Brand: Samsung Model: Galaxy S8 (SM-G950FD) Serial no: RF8J709YX6B MAC address: 30:07:4D:E1:3C:44</p> <p>Brand: ASUS Model: ASUS_X008D Serial no: 354224086418942 MAC address: 70:4D:7B:AD:FD:7F</p> <p>Brand: Firefly Mobile Model: Aurii Secret Lite Serial Number: PFCUSSKFSKHYDMWC MAC Address: 00:90:55:33:35:68</p>

III. Impact of the request fulfillment (Brief Description)					
<p>IT Operations Infrastructure: Mobile Phone, Mobile Web Browsers</p> <p>IT Security Infrastructure: Firewall</p> <p>IT Operations Security Policy:</p>					
<table border="1"> <tr> <td rowspan="2">  </td> <td>Proprietary and Confidential</td> <td>Page 1 of 2</td> </tr> <tr> <td></td> <td>Template Version : 01</td> </tr> </table>		Proprietary and Confidential	Page 1 of 2		Template Version : 01
		Proprietary and Confidential	Page 1 of 2		
		Template Version : 01			

Process Owner: IT Operations	FORM	F-ITO-SEC-1.1
	Security Exception Request	

5.2 Internet Usage Policy under PPM-ITO-SEC-1.0 - Corporate Information Security Policies

IV. Potential IT Operational Risk

- Device Attacks such as Browser-based attacks and exploitations
- Mobile malware thru social media sites, shared links and rogue applications
- Leakage of company data and information
- Phishing
- Risk of client information leakage due to it being contained in a non-company owned/controlled mobile device

V. Risk Response Method to be used

Risk Mitigation: Mobile phone has to be connected to OAMPI wifi which isolates the access to the Internet only – user won't be able to access Internal resources.

User is only permitted to use OAMPI WiFi access during business hours and extended hours as approved by her immediate superior.

User shall delete any confidential and/or client information that maybe contained in the phone through the use of OAMPI WiFi after the validity period of the request.

User mobile phone will be subject to the Corporate Information Security Policies of Open Access BPO as an IT asset which will be monitored by the IT Operations during the validity period of the request.

VI. IT Operations Endorsement

Name and Signature:

Marlon De Guzman

Date:

June 26, 2018

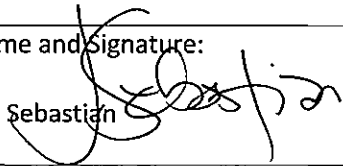
VII. Business Justification and validity period of security exception

CirclesLife clients requested that the operations team be added to CL internal groups using Whatsapp that will help us be updated and informed of the latest in operations, promotions and roadshows. We will also receive urgent updates, program specific KPIs especially CSAT, and escalation updates. There will be images shared when there would updates or reports of tools or issues.

VIII. Top Management Representative Approval

	Proprietary and Confidential		Page 2 of 2
			Template Version : 01

Process Owner: IT Operations	FORM	F-ITO-SEC-1.1
	<i>Security Exception Request</i>	

Name and Signature:  Joy Sebastian	Date:
---	-------

IX. Information Security Team Approval (If applicable)	
Name and Signature:	Date: