UGANDA NATIONAL COMPUTER EMERGENCY RESPONSE TEAM (CERT.UG)

18 March 2020

PANDEMIC PREPAREDNESS ADVISORY

The global impact of COVID-19 which was declared a pandemic by the World Health Organisation (WHO) raises the need for organisations to review business continuity plans especially due to the impact on both staff and third party services. Due to its contagious nature, global reports estimate that an organization in an affected area may experience a significant increase in employee absenteeism due to medical reasons or prevention measures. This would be the same effect for service providers that your organization relies on for critical Information Technology (IT) services.

Based on the above, the Uganda National Computer Emergency Response Team and Coordination Center strongly urges all organisations to review and prepare response plans first to protect staff as well as ensure continuity of critical IT enabled services. As per the best practice in cybersecurity, all response plans should be risk based in order to ensure presence of appropriate mitigation measures. In line with this, the following approach should be used:

a) Increase internal communications to raise staff awareness on the COVID-19 pandemic using guidance from the Ministry of Health
b) Conduct Business Impact Assessments of IT enabled services to determine the most critical and their dependencies
c) Identify the staff and contract or third party staff required to maintain the identified critical IT enabled services
d) Ensure backup and recovery procedures are current and tested. Make sure third parties that provide critical IT services are engaged to provide you with their response plans in line with this current pandemic. Communication and collaboration across in house and external support teams is crucial.
e) Identify incident management teams that are trained and capable of fulfilling various roles and functions. Each team member should have a copy of the updated

response plan that includes an escalation matrix and contacts (phone, skype ids, etc) for persons supporting each critical IT enabled service

f) Prepare for increase in use of remote access to IT services using VPN. If your critical IT staff are to work from home, the organization has to facilitate remote access bandwidth requirements such as increasing data plans or providing modems with sufficient capacity with the appropriate network security controls.
g) Prepare to increase monitoring of IT enabled services in order to quickly identify any anomaly or suspicious activity
h) Prepare to provide IT support and guidance for staff that may have to work from home in the event this happens (The global average is that 25% - 50% of staff depending on the prevailing circumstances, will be absent from work as a safety measure or due to medical reasons or taking care of vulnerable people). This should include options of using teleconferencing and video conferencing solutions in line with organizational policies with the appropriate security controls.

In any situation, preparedness is always the best response to survivability.

All organisations are therefore advised to follow through the above to increase resilience during this pandemic outbreak period.

Uganda National Computer Emergency Response Team
Plot 7A, Rotary Avenue (Former Lugogo Bypass)
Twitter: @CERT.UG | Facebook: Cert1.ug
info@cert.ug
www.cert.ug