Global Cybersecurity Resource
CSOC POSTMORTEM INCIDENT REPORT

Prepared (also subject responsible if other)		No		
Adefemi Debo-Omidokun				
Approved	Checked	Date	Rev	Reference
Brian Hurley		2017-11-03	V1	

Client Name	**Mandatory**
CSOC Analyst Name	**Mandatory**
Incident Slogan	**Mandatory**
GCR Incident Reference/TT #	**Mandatory**
Ticket Priority	**Mandatory**
Target System (IP/MAC?)	**Mandatory**
3rd Party involved and TT Reference	**Mandatory**
Teams involved in Incident	**Mandatory**
Executive Summary	On the XXth XXXember 201X at 11:04 EST, customer XXX experienced a cyber attack/intrusion/disruption.....impacting xxxxxxxxxxxx area of the network/business. Investigation revealed: XXXXXXXXXX All services were restored on <Date> at 12:28 EST. Total outage/impact duration was XX Minutes **Mandatory** including: *-Fault occurrence date and time* *-Who detected it and how* *-What was the impact in network and services* *-What was the RFO* *-Recovery actions and who performed it* *-Fault clearance date (if other date than the fault start) and time*
Incident Timelog	xx-xx-201x 11:04 EST
Time Alarm/Attack Generated	xx-xx-201x 11:12 EST
Date & Time Ticket Created	xx-xx-201x 12:28 EST

Prepared (also subject responsible if other)		No		
Adefemi Debo-Omidokun				
Approved	Checked	Date	Rev	Reference
Brian Hurley		2017-11-03	V1	

Date & Time Service Up & Running	xh:xxm
Incident Lead Time (Time alarm/intrusion attempt generated – service up and running)	**Mandatory**
Reason(s) for incident exceeding the Lead Time (SLA)?	

I. Impact on Customer

Client Impact	**Mandatory – Ex.** *Client's located at …. province/area have experienced no or ...*
Number of End Users Impacted	**Mandatory in terms of number of users/equipment affected and technology**
Affected Business Area	**Mandatory**

II. Impact on Services

Affected Services	**Mandatory**

III. Reason for Outage

PO (Previous Occurrence) reference	**Mandatory**
Root Cause Description	**Mandatory**
Permanent Solution Applied	**Mandatory**
Interim Workarounds	**Mandatory**

IV. Methods of Improvement - Short term / long term

Prepared (also subject responsible if other)		No		
Adefemi Debo-Omidokun				
Approved	Checked	Date	Rev	Reference
Brian Hurley		2017-11-03	V1	

Domain/Service area	Description
Methods to Improve Detection of Problem	**Mandatory**
Methods to Improve Incident Lead Time	**Mandatory**
Methods to Prevent Future Related Outages	**Mandatory**
Improvement Plan/Change Required for this failure?	**Mandatory**

V. Action Points

Description	Action Owner	Due Date

VI. Other