CENTRAL BANK OF TRINIDAD & TOBAGO

CYBER INCIDENT REPORTING

Particulars and Details of Incident	
Name of Financial Institution:	
Reporting Officer's Name:	
Reporting Officer's Position:	
Reporting Officer's Email & Phone Number:	
Date and Time of Notification:	
Date and Time Incident Discovered / Detected:	
Incident Level or Priority:	
Type of Incident that occurred (e.g. Ransomware, Phishing, Data Breach / Leak, Insider Threat, DDoS):	
Current state of incident:	
Indicate Actions Taken:	
Impact Assessment (examples are given but not exhaustive)	
Business Lines Impacted (including availability of services – Treasury Services, Cash Management, ATM, Internet / Mobile Banking, etc.):	
Stakeholders Impacted:	
Financial and Market Impact (trading activities, liquidity impact, transaction volumes and values etc.):	
Reputational Impact:	
Detailed chronological order of events	
Date of Incident, Start Time and Duration (DD/MM/YY)	
Escalation Steps Taken:	
Stakeholders Informed or Involved:	
Channels of Communication Involved:	
Root Cause Analysis	
Factors that caused the problem / reason for occurring:	
Interim measures to mitigate / resolve the issue**:**	

CENTRAL BANK OF TRINIDAD & TOBAGO

CYBER INCIDENT REPORTING

Final Assessment and Remediation	
Actions completed and pending:	
Conclusion on cause and effects of incident:	
Provide the Indicators of Compromise (IOCs):	
List the corrective actions taken to prevent future occurrences of similar types of incident:	
Estimated timelines to address the remediation of the incident (DD/MM/YY)	