**Incident Report Template**

Instructions:

1. **Incident or Immediate Notification to MAS (as soon as possible, within an hour):** 
   * Submit Section (A); and
   * Submit Annex, if it is a cyber-security incident.
2. **Subsequent update(s) to MAS (updates to be provided as and when there are changes in the current situation, or as requested by MAS):**
   * Submit any updates to Section (A); and
   * Submit any updates to Annex, if it is a cyber-security incident.
3. **Full Incident Report to MAS (as required under the relevant legislation) :**
   * Submit Section (A) and (B).

|  |  |
| --- | --- |
| **Section (A) Items 1 to 3** | |
| 1. **Particulars:** |  |
| * Date and Time of Notification to MAS |  |
| * Full Name of Institution |  |
| * Name of Caller/Reporting Staff |  |
| * Designation/Department |  |
| * Contact details (e.g. email, mobile) |  |
| 1. **Details of Incident:** |  |
| * Discovery date and time of incident |  |
| * Type of incidents, affected areas:  1. **Outage of IT system** (e.g. core banking systems, ATMs, payment systems such as EFTPOS, CTS, GIRO, MEPS+, CLS)? 2. **Cyber Security Incident** *(e.g. hacking, web defacement)?* ***[Please complete Annex]*** 3. **Theft or Lost of Information***(e.g. sensitive/important/customer information stolen or missing from business locations)?* 4. **Outage of Infrastructure** *(e.g. which premises, power/utilities, telecommunications, fire)?* 5. **Financial** *(e.g. liquidity, bank run)?* 6. **Unavailability of Staff** (e.g. number and percentage on loss of staff or staff absenteeism (for pandemics, FIs are to provide breakdown by infection, quarantine, suspected and absent)? 7. **Others** *(e.g. outsourced service providers, breach of laws and regulations)?* |  |
| * What actions or responses have been taken by the institution? |  |
| 1. **Impact Assessment(examples are given but not exhaustive):** |  |
| * Business impact including availability of services – Treasury Services, Cash Management, Trade Finance, Branches, ATMs, Internet Banking, Clearing and Settlement activities etc |  |
| * Stakeholders impact – affected retail/corporate customers, affected participants including operator, settlement institution and service providers etc |  |
| * Financial and market impact – Trading activities, transaction volumes and values, monetary losses, liquidity impact, bank run, withdrawal of funds etc |  |
| * Regulatory and Legal impact |  |
| **Section (B) Items 4 to 6** | |
| 1. **Detailed chronological order of events:** |  |
| * Date of incident, start time and duration. |  |
| * Escalation steps taken, including approvals sought on interim measures to mitigate the event, and reasons for taking such measures |  |
| * Stakeholders informed or involved |  |
| * Various channels of communications involved |  |
| * Rationale on the decision/activation of BCP and/or IT DR |  |
| 1. **Detailed Root Cause Analysis:** |  |
| * Factors that caused the problem/ Reasons for occurring |  |
| * Interim measures to mitigate/resolve the issue, and reasons for taking such measures, and |  |
| * Steps identified or to be taken to address the problem in the longer term. |  |
| 1. **Final assessment and remediation:** |  |
| * Conclusion on cause and effects of incident |  |
| * List the corrective actions taken to prevent future occurrences of similar types of incident |  |
| * Target date of resolution\_\_\_\_\_\_\_\_\_(DD/MM/YY). |  |

**Annex**

Note: All fields are REQUIRED to be filled unless otherwise stated.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NATIONAL CYBER SECURITY INCIDENT REPORTING FORM** | | | | |
| **Section A: General Information Ref No:** | | | | |
| A1. Sector :  Banking & Finance | | | | |
| A2. Reporter's Contact Information: *(Please provide if different from Section (A) Item 1)* | | | | |
| Organization: |  | | | |
| Name: |  | | | |
| Appointment: |  | | | |
| Email Address: |  | | | |
| Telephone Number: |  | | | |
| A3. Is this a New incident Update to reported incident?   * For the first update, please indicate “1. If this is an update to a reported incident, please provide the sequence number for this update.   Sequence No: Click here to enter text. | | | | |
| A4. What category is this incident being classified as? | | | | |
| Category 1  Affected critical system | | Category 2  Incident occurred on  system or network that  could put the critical system at risk | Category 3  Incident occurred on non-critical system | |
|  | | | | |
| **Section B: Incident** | | | | |
| B1. When was the incident reported to the Sector Lead i.e. MAS?  (Please specify in Singapore Local Time (+8GMT))  Date: Click here to enter a date. | | | | |
| B2. Types of Threat/Incident  (You may choose more than one item)  Denial of Service (DoS)  Distributed Denial of Service (DDoS)  Virus/Worm/Trojan  Intrusion/Hack/Unauthorised access  Website Defacement  Misuse of Systems/Inappropriate usage  Other: Click here to enter text. | | | | |
| B3. Is this incident related to another incident previously reported?  Choose an item.   * If “Yes”, provide more information on how both incidents are related.   Click here to enter text.   * Please provide the reference no. of the previously reported incident.   Ref no: Click here to enter text. | | | | |
| **Section C: Incident Details** | | | | |
| C1. Please provide details of the incident in the box below.   * When was the incident first observed?   Click here to enter a date.   * How was the incident first observed/sighted/detected?   Click here to enter text.  C2. Please provide details of the critical system(s) or network(s) that is/are impacted by this incident. Details should minimally include:  -*Location, purpose of this system/ network, affected applications (including hardware manufacturer, software developer, make/ model, etc) running on the systems/ networks, etc.*  Click here to enter text.  Where relevant, please indicate the Operating System of the affected critical system(s): Choose an item.   * If others, kindly state the OS: Click here to enter text.   C3. What is the impact of the attack? (*Tick ‘one’ checkbox for each column*)   |  |  |  | | --- | --- | --- | | Service Delivery | (Loss of ) Sensitive Information | Public Confidence and Reputation | | No Impact | No loss | No Impact | | Minor Impact | Minor Loss | Minor Impact | | Major Impact | Major Loss | Major Impact | | Serious Impact | Serious Loss | Serious Impact | | Severe Impact | Severe Loss | Severe impact |   C4. Does the affected critical system(s)/ network(s) have potential impact to another critical asset(s) of the financial institution?  Choose an item.   * If “Yes”, please provide more details.   Click here to enter text. | | | | |
| **Section D: Incident Handling Status** | | | |
| D1. What is/are the type(s) of follow up action(s) that has/have been taken at this time?  Click here to enter text.  D2. What is the current status or resolution of this incident?  Choose an item.  If it is not resolved, what is the next course of actions?  Click here to enter text.  D3. What is the earliest known date of attack or compromise? *(Tick ‘checkbox’ if unknown)*  (Please specify in Singapore Local Time +8GMT)  Date: Click here to enter a date. Unknown:  D4. What is the source/cause of the incident? *(‘NIL’ OR ‘NA’ if unknown)*  Click here to enter text.  D5. Has the incident been reported to any law enforcement?  Choose an item.   * If “Yes”, specify the agency that is being reported to.   Click here to enter text.. | | | |
| **Section E: Other Information** | | | |
| E1. IP addresses(*Required if surfaced from the incident*)  Provide the list of IP addresses surfaced from incident. Please state the involvement of the IP addresses in the incident (eg. Victim, Malware Command & Control Servers, etc). If IP addresses were resolved from domain names, please specify the domain names and the date/time of resolution of IP addresses from the domain names.   |  |  |  |  | | --- | --- | --- | --- | | IP Address | Involvement | Domain name from which IP address was resolved | Date/Time of Resolution of IP address from Domain name | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |   E2. Domain Names (*Required if surfaced from the incident*)  Provide the list of domains surfaced from incident. Please state the involvement of the domain names in the incident. (eg. Drive-by-download Servers, Malware Control & Command Servers, defaced website)   |  |  | | --- | --- | | Domain Name | Involvement of Domain name | |  |  | |  |  | |  |  | |  |  |   E3. Email addresses (*Required if surfaced from the incident*)  Provide list of email addresses surfaced from incident. Please state the involvement of the email addresses in the incident. For example, email address from which a phishing email appeared to be sent from, etc.   |  |  | | --- | --- | | Email Address | Involvement of Email Address | |  |  | |  |  | |  |  | |  |  | |  |  |   E4. Malicious files (*Required if surfaced from the incident*)  Provide information on the malicious files surfaced in the incident in the box below.   |  |  |  |  | | --- | --- | --- | --- | | Filename | Size | MD5 hash | Technical Analysis (Yes/No) | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | | | | |