# Incident Reporting Template

Instructions:

|  |  |  |
| --- | --- | --- |
|  | **All Incidents** | **For Cyber Security Incidents Only** |
| **1. Incident Notification to MAS (as soon as possible, within an hour)** | * Submit Section (A) of this Incident Reporting Template | **For CII institutions**:   * To also submit the National Cyber Security Incident Reporting Form available from the Cyber Security Agency of Singapore (CSA) website, or via the link here:   <https://www.csa.gov.sg/legislation/forms>  **For all other FIs**:   * To also submit Annex in this Incident Reporting Template |
| **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) | **For CII institutions**:   * Submit any updates to the National Cyber Security Incident Reporting Form   **For all other FIs**:   * Submit any updates to the Annex |
| **3. Full Incident Report to MAS**  **(as required under the relevant legislation)** | * Submit Section (A) and (B) | |

**For suspicious activities and incidents of fraud that are material to the safety, soundness or reputation of the FI, the FI shall submit Form F1 set out in the respective Notices listed below to MAS no later than 5 working days upon the discovery of such activity or incident by post, fax or encrypted email, as required in the relevant notice.**

* **MAS Notice 1120 under the Banking (Amendment) Act 2020**
* **MAS Notice 641 under the Banking Act (Cap. 19)**
* **MAS Notice PSN03 under the Payment Services Act 2019 (Act 2 of 2019)**

|  |  |
| --- | --- |
| **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 |  |
| * Nature of incidents, affected areas:  1. **Outage of IT system** (*e.g. core banking systems, ATMs, payment systems such as EFTPOS, CTS, GIRO, MEPS+, CLS etc)* 2. **Signs of cyber-attack** *(e.g. Hacking or malware infection against FI’s system, web defacement, distributed denial of service attacks)?* ***[Please complete Annex]*** 3. **Theft or Loss of Information** *(e.g. sensitive/important/customer information stolen or missing from business locations)* 4. **Unavailability of Infrastructure or work premises** *(e.g. Power blackout, telecommunication linkages down, fire in office building and the affected locations.)?* 5. **Financial** *(e.g. liquidity, bank run)?* 6. **Unavailability of Staff** *(e.g.* *High absenteeism or loss of staff affecting BAU due to infectious diseases, physical attack, prolonged MRT breakdowns leading to BCP activation etc)?* 7. **Others** (e.g. *Unavailability of 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. |  |
| * Reputational impact – is incident likely to attract media attention? |  |
| * 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 (for non-CII institutions)** | |
| **Section A: General Information Ref No:** | |
|  | |
| A1. Reporter's Contact Information: *(Please provide if different from Section (A) Item 1)* | |
| Organization: |  |
| Name: |  |
| Designation: |  |
| Email Address: |  |
| Telephone Number: |  |
| A2. Is this a New incident Update to reported incident?   * For new incident, to provide an internal reference number (if any).   Reference No: Click here to enter text.   * If this is an update to a reported incident, please provide the sequence number for this update.   Sequence No: Click here to enter text. | |
| **Section B: Incident Details** | |
| Please specify in Singapore Local Time GMT+8, for B1, B2 and B3 below:  B1. When did the institution become aware of the incident?  Date: Click here to enter text.  Time: Click here to enter text.  B2. When was the incident reported to MAS?  Date: Click here to enter text.  Time: Click here to enter text.  B3. Based on the institution’s understanding of the incident, when did it occur?  Date: Click here to enter text.  Time: Click here to enter text.  Unknown   * If “Unknown”, when was the incident first observed/sighted/detected?   Date: Click here to enter text.  Time: Click here to enter text.  B4. Based on the institution’s understanding of the incident, how was the incident first observed/sighted/detected?  Click here to enter text.  B5. 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. | |
| B5. 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  Others: Click here to enter text. | |
| B6. 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 |   B7. Does the affected critical system(s)/ network(s) have potential impact on another critical asset(s) of the financial institution?  Choose an item.   * If “Yes”, please provide more details.   Click here to enter text.  B8. 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 Handling Status** | |
| C1. What is/are the type(s) of follow up action(s) that has/have been taken at this time?  Click here to enter text.  C2. What is the current status or resolution of this incident?  Choose an item.  C3. If it is not resolved, what is the next course of actions?  Click here to enter text.  C4. 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:  C5. What is the source/cause of the incident? *(‘NIL’ OR ‘NA’ if unknown)*  Click here to enter text.  C6. Has the incident been reported to any law enforcement agencies?  Choose an item.   * If “Yes”, specify the agency that is being reported to.   Click here to enter text. | |
| **Section D: Other Information** | |
| D1. IP addresses  Provide the list of IP addresses surfaced from incident. Please state the involvement of the IP addresses in the incident (e.g. 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  Provide the list of domains surfaced from incident. Please state the involvement of the domain names in the incident. (E.g. Drive-by-download Servers, Malware Control & Command Servers, defaced website)   |  |  | | --- | --- | | **Domain Name** | **Involvement of Domain name** | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  |   E3. Email addresses  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  Provide information on the malicious files surfaced in the incident in the box below.   |  |  |  |  | | --- | --- | --- | --- | | **Filename** | **Size** | **MD5 hash** | **Technical Analysis (Yes/No)** | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | | |