# **Annex A: IT & Cyber Incident Initial Report Template**

## 

## **Section 1: Contact Particulars and Incident Reference**

|  |  |
| --- | --- |
| 1. **Contact Particulars and Incident Reference** | |
| Registered Name of Firm | [ Click here to add text] |
| Name of Reporting Staff | [ Click here to add text] |
| Designation/Department | [ Click here to add text] |
| Contact Number | [ Click here to add text] |
| Contact Email | [ Click here to add text] |
| Incident Reference Number  (Date of first report YYYYMMDD + 9-digit License Number e.g., 20240101000001001) | [ Click here to add text] |

## **Section 2: Incident Details**

The section below should be completed with the most up-to-date information available to the firm. Where applicable, the firm may provide additional information as attachments to support the descriptions.

| 1. **Incident Details** | |
| --- | --- |
| 1. Discovery date and time  (w*hen did the firm become aware that an incident had taken place*). | [ Click here to add text] |
| 1. Describe how the incident was discovered (e.g., *malware was detected by a security monitoring alert, staff noticed anomalous transactions customer complaint, ransom note, etc.*) | [ Click here to add text] |
| 1. Describe the nature of the incident and the systems affected (*more than one option can be applicable*)  * Unscheduled system outage/disruption arising from internal lapses or unforeseen hardware/ software failures (*e.g., system misconfiguration, power outage, etc.*). * Cyber-attack by known/ unknown threat actor(s) (*e.g., ransomware with extortion demand, DDoS attack, etc.*). Provide any shareable intelligence on the cyber-attack (*e.g., attacker IP address, domain name, malware hash, indicators of compromise, etc.*) * Data leak or compromise (*e.g., data exfiltration by threat actor(s), control lapse resulting in customer information made public, etc.*) * Others. | [ Click here to add text] |
| 1. Is the firm aware of any contagion effect the incident may have on the ADGM or other ADGM firms  (*e.g., malware spread through network connection, etc.*)? | [ Click here to add text] |
| 1. Describe the nature (e.g. *financial, operational, reputational, legal, regulatory, other)* and the degree (severe, moderate, mild) of impact of the incident on the firm. | [ Click here to add text] |
| 1. Describe the impact of the incident on the business operations and services to customers and whether there has been any suspension to the firm’s business or any of its activity. | [ Click here to add text] |
| 1. Describe any impact on customers (financial loss, data leakage, limited access etc.) and any actions taken to limit such impact. | [ Click here to add text] |
| 1. Describe the actions taken thus far to contain the incident operationally. (*e.g., workstation disconnected from internet, cyber incident response vendor engaged, customer communications, etc.*) | [ Click here to add text] |
| 1. Describe any reporting (including date and time of report) made to federal authorities, law enforcement agencies, local & foreign regulators, etc. (*e.g., FIU, Commissioner of Data Protection, Abu Dhabi Police, etc.*). | [ Click here to add text] |
| 1. Describe any media / social media coverage of the incident. | [ Click here to add text] |