MFSA MALTA FINANCIAL SERVICES AUTHORITY

Major ICT-Related Incident Report
Instructions

Major ICT-Related Incident Report
Instructions

1. Licence Holders / Authorised Persons should fill out the relevant section of the template, depending on the reporting phase they are in: Section / Sheet A for the Initial Report, Section / Sheet B for Intermediate Reports and Section / Sheet C for the Final Report. The same file should be used when submitting the Initial, Intermediate and Final Reports related to the same Major ICT-Related Incident. **All fields are mandatory, unless it is clearly specified otherwise.**

2. Please Select the Type of Report:

Type of Report		
A - Initial Report	☐	The Initial Report (Section / Sheet C) is the first notification that the Licence Holder / Authorised Person submits to the Malta Financial Services Authority (MFSA) within **four (4) hours** after a Major ICT-Related Incident is classified as Major. Incidents should be classified as Major within **twenty-four (24) hours** after they are detected.
B - Intermediate Report	☐	The Intermediate Report provides a more detailed description of the Major ICT-Related Incident and its consequences and is to be submitted within **three (3) working days** from the submission of the Initial Report. It updates the Initial Report (and where applicable, a previous Intermediate Report) on the same Incident. It informs the MFSA that regular activities have been recovered and business is back to normal.
C - Final Report	☐	The Final Report is the last report sent on the Incident since: i) a root cause analysis has already been carried out and estimations can be replaced with real figures; or ii) the Incident is not considered major anymore and need to be reclassified because it no longer meets the threshold to be considered major and is not expected to fulfil it before it is resolved. This is to be submitted within **twenty (20) working days** from the submission of the Intermediate Report.

MFSA MALTA FINANCIAL SERVICES AUTHORITY

Major ICT-Related Incident Report

Initial Report

Major ICT-Related Incident Report
A - Initial Report

Note: The Initial Report is to be submitted within **four (4) hours** after classifying an ICT-Related Incident as Major. Incidents should be classified as Major within **twenty-four (24) hours** after they are detected. An explanation is to be provided within the space available below if the Licence Holder / Authorised person required longer than twenty-four (24) hours.

A0.1 Report Date and Time	**Date** (dd/mm/yyyy)	
	Time (hh:mm)	
A0.2 Incident Reference Number		

A1 - General Details

A1.1 Licence Holder / Authorised Person Name *(as per MFSA Financial Services Register)*	
A1.2 Licence Holder / Authorised Person Identification (*as per MFSA Financial Services Register*)	
A1.3 Company Registration Number (*MBR*)	

A1.4 Licenced/Authorised Activities Affected by the Incident *(select where applicable)*

- ☐ **Company Service Provider**
- ☐ **Compensation Scheme**
  - ☐ Depositor Compensation Scheme
  - ☐ Investor Compensation Scheme
- ☐ **Credit Institution**
  - ☐ Credit Institution
  - ☐ Credit Intermediary
- ☐ **Financial Institution**
- ☐ **Insurance**
  - ☐ Insurance Undertaking
  - ☐ Insurance Intermediary
- ☐ **Pensions**
  - ☐ Retirement Schemes - Personal
  - ☐ Retirement Schemes - Occupational
  - ☐ Service Provider
  - ☐ Retirement Fund
- ☐ **Securities and Markets**
  - ☐ Investment Firm
  - ☐ Fund Manager
  - ☐ Custodian / Depositary
  - ☐ Fund
  - ☐ Recognised Person
  - ☐ Trading Venue
  - ☐ Central Securities Depository
  - ☐ Data Reporting Service Provider
  - ☐ Securitisation
  - ☐ Capital Market
  - ☐ Market Oversight
  - ☐ Crowd Funding
- ☐ **Trustees and Other Fiduciaries**
- ☐ **Virtual Financial Assets**
- ☐ **Other** — **Please specify** *(if more than one Activity please separate each Activity with a comma)*

A1.5 Head of Group (N/A *if not applicable*)	
A1.6 Head of Group Country of Establishment (N/A *if not applicable*)	

A1.7 Country/ies Affected by the Incident (select *where applicable*)

☐ **AT** *Austria*	☐ **EE** *Estonia*	☐ **IE** *Ireland*	☐ **PL** *Poland*
☐ **BE** *Belgium*	☐ **EL** *Greece*	☐ **IT** *Italy*	☐ **PT** *Portugal*
☐ **BG** *Bulgaria*	☐ **ES** *Spain*	☐ **LT** *Lithuania*	☐ **RO** *Romania*
☐ **CY** *Cyprus*	☐ **FI** *Finland*	☐ **LU** *Luxembourg*	☐ **SE** *Sweden*
☐ **CZ** *Czechia*	☐ **FR** *France*	☐ **LV** *Latvia*	☐ **SI** *Slovenia*
☐ **DE** *Germany*	☐ **HR** *Croatia*	☐ **MT** *Malta*	☐ **SK** *Slovakia*
☐ **DK** *Denmark*	☐ **HU** *Hungary*	☐ **NL** *Netherlands*	
☐ **CH** *Switzerland*	☐ **IS** *Iceland*	☐ **LI** *Liechtenstein*	☐ **NO** *Norway*

☐ **GB** *United Kingdom of Great Britain and Northern Ireland*

☐ **Other** — **Please specify** *(if more than one other country, please separate each country name with a comma)*

A1.8 Primary Contact Person	**Name**	
	Surname	
	Designation	
	Email Address	
	Direct Land Line	
	Mobile	
A1.9 Secondary Contact Person	**Name**	
	Surname	

Designation	
Email Address	
Direct Land Line	
Mobile	

A2 - Incident Detection and Classification

A2.1 Incident Detection Date and Time	Date (dd/mm/yyyy)	
	Time (hh:mm)	
A2.2 Incident Classification Date and Time	Date (dd/mm/yyyy)	
	Time (hh:mm)	
A2.3 Incident Detection Mechanism	Please Select	
	If Other Please Specify	

A2.4 Incident Type

☐ Security ☐ Operational

A2.5 Criteria for Classifying an ICT-Related Incident as Major

☐ Transactions Affected ☐ Service Downtime ☐ Economic Impact ☐ Other Licence Holders / Authorised Persons / Relevant Infrastructures Affected

☐ Users Affected ☐ Breach of Security ☐ High Level of Internal Escalation

☐ Geographical Spread ☐ Reputational Impact

A2.6 A Short and General description of the Incident

A2.7 Impact in other EU Member States
(N/A if not applicable)

A2.8 Reporting to other Authorities

☐ *Yes* ☐ *No*

If Yes Please Specify	

A2.9 Reasons for Late Submission
(N/A if not applicable)

MFSA MALTA FINANCIAL SERVICES AUTHORITY

Major ICT-Related Incident Report
Intermediate Report

Major ICT-Related Incident Report
B - Intermediate Report

Note:
- If this is not the Intermediate Report being submitted, please leave this sheet completely blank;
- The Intermediate Report is to be submitted within **three (3) working days** from the submission of the Initial Report.

B0.1 Report Date and Time	**Date** (dd/mm/yyyy)	
	Time (hh:mm)	
B0.2 Incident Reference Number		

B1 - General Details

B1.1 Changes Made in Sheet *A - Initial Report* (Question Numbers Only) (if more than one question, please separate each question number with a comma; *N/A if not applicable*)	
B1.2 Description of the Changes Made in *Sheet A - Initial Report* (*N/A if not applicable*)	
B1.3 What is/was the Specific Issue?	
B1.4 How did the Incident Start?	
B1.5 How did it Evolve?	
B1.6 Was it related to a previous incident?	☐ *Yes* ☐ *No*
If Yes Provide	
If No Reference Number Please Specify	
B1.7 Were Other Licence Holders / Authorised Persons / Third Parties Affected or Involved?	☐ *Yes* ☐ *No*
If Yes	
B1.8 Incident Start Date and Time	**Date** (dd/mm/yyyy)
	Time (hh:mm)
B1.9 Has the Incident been Resolved?	☐ *Yes* ☐ *No*
If **Yes** Provide Date and Time If **No** Provide Estimate Future Date and Time	**Date** (dd/mm/yyyy) **Time** (hh:mm)

B2 - Incident Classification and Impact

B2.1 Incident Classification

☐ **Transactions Affected** Number of Transactions % of Regular Number of Transactions Value of Transactions (EUR) Duration (hh:mm)	☐ **Service Downtime** Duration (hh:mm)	☐ **Economic Impact** ☐ **Geographical Spread**	☐ **Other Authorised Persons / Financial Entities / Relevant Infrastructures Affected** Please describe:
☐ **Users Affected** Number of Users % of overall users	☐ **Breach of Security Measures** ☐ Logical Security ☐ Physical Security ☐ ICT Operations Security	☐ **High Level of Internal Escalation** Please describe:	☐ **Reputational Impact** Please describe:

☐ Security Monitoring

☐ **Other** — **Please specify**

Additional Comments

☐ **Still Under Investigation** (*Information to be provide in an another Intermediate Report*)

B2.2 Overall Impact

☐ **Confidentiality** ☐ **Integrity** ☐ **Availability** ☐ **Authenticity**

- ☐ Sensitive Entity Data Leaked
- ☐ Sensitive User Data Leaked

B2.3 Financial Services Affected

B2.4 What are the Consequences? (in particular for users)

B3 - Incident Description

B3.1 Incident Type

B3.2 Root Cause

Secruity

Malicious Action

- ☐ **Abusive Content**
- ☐ **Web Defacement**
- ☐ **Malicious Code**
  - ☐ Virus
  - ☐ Worm
  - ☐ Trojan
  - ☐ Spyware
  - ☐ Dialler
  - ☐ Rootkit
- ☐ **Information Gathering**
  - ☐ Scanning
  - ☐ Sniffing
  - ☐ Social Engineering
- ☐ **Intrusions**
  - ☐ Privileged Account Compromise
  - ☐ Unprivileged Account Compromise
  - ☐ Application Compromise
  - ☐ Bot
- ☐ **Availability**
  - ☐ DOS
  - ☐ DDOS
- ☐ **Deliberate Internal Actions**
  - ☐ Sabotage
  - ☐ Theft
- ☐ **Deliberate External Physical Damage**
  - ☐ Sabotage
  - ☐ Physical Attack of Premises
- ☐ **Information Content Security**
  - ☐ Unauthorised Access to Information
  - ☐ Unauthorised Modification of Information
- ☐ **Fraudulent Actions**
  - ☐ Unauthorised Use of Resources
  - ☐ Copyright

Operational

Process Failure

- ☐ **Deficient Monitoring and Control**
- ☐ **Communication Issues**
- ☐ **Improper Operations**
- ☐ **Inadequate Change Management**
- ☐ **Inadequacy of Internal Procedures and Documentation**
- ☐ **Recovery Issues**
- ☐ **Other** (use space below)

System Failure

- ☐ **Hardware Failure**
- ☐ **Network Failure**
- ☐ **Database Issues**
- ☐ **Software / Application Failure**
- ☐ **Physical Damage**
- ☐ **Other** (use space below)

Human Error

- ☐ **Unintended**
- ☐ **Inaction**
- ☐ **Insufficient Resources**
- ☐ **Other** (use space below)

- ☐ Masquerade
- ☐ Phishing
- ☐ **Advanced Persistent Threat** (Please indicate number in space provided for Other)
- ☐ **Other** (use space below)

☐ **External Event**

☐ **Failure of supplier / technical service provider** ☐ **Force Majeure** ☐ **Other** (use space below)

☐ **Other** — Please specify *(please indicate whether Malicious Action, Process Failure, System Failure, Human Error, External Event, or Other)*

☐ **Still Under Investigation** (*Information to be provided in an another Report*)

B3.3 Was the Incident Affecting you Directly, or Indirectly through a Service Provider

☐ ***Directly*** ☐ ***Indirectly***

If **Indirectly** Please Provide the **Name** of the **Service Provider**

B4 - Incident Response and Mitigation

B4.1 Which actions/measures have been taken so far or are planned to recover from the incident?

B4.2 Was Crisis Management started (internal and/or external)?

☐ ***Yes*** ☐ ***No***

If Yes

B4.3 Was the Incident communicated to the users?

☐ ***Yes*** ☐ ***No***

If Yes

B4.4 Has the Business Continuity Plan and/or Disaster Recovery Plan been activated?

☐ ***Yes*** ☐ ***No***

If **Yes** Provide Date and Time
If **No** Provide Estimate Future Date and Time

Date (dd/mm/yyyy)

Time (hh:mm)

If Yes Please Describe

MFSA MALTA FINANCIAL SERVICES AUTHORITY

Major ICT-Related Incident Report
Final Report

Major ICT-Related Incident Report
C - Final Report

Note:
- If this is not the Final Report being submitted, please leave this sheet completely blank;
- The Final Report is to be submitted within **twenty (20) working days** after business is deemed back to normal;
- Sheet *B - Intermediate Report* should be fully completed and updated as part of the submission of the Final Report whether an Intermediate Report has already been submitted or not except in the circumstance whereby an incident is re-classified back to non-Major.

C0.1 Report Date and Time	**Date** (dd/mm/yyyy)	
	Time (hh:mm)	
C0.2 Incident Reference Number		
C0.3 Incident Re-classified back to Non-Major	☐ *Yes* ☐ *No*	
	If Yes Please	

C1 - General Details

C1.1 Changes Made in Sheet *A - Initial Report* (Question Numbers Only) (if more than one question, please separate each question number with a comma; *N/A if not applicable*)	
C1.2 Description of the Changes Made in *Sheet A - Initial Report* (*N/A if not applicable*)	
C1.3 Changes Made in Sheet *B - Intermediate Report* (Question Numbers Only) (if more than one question, please separate each question number with a comma; N/A if not applicable)	
C1.4 Description of the Changes Made in Sheet *B - Intermediate Report* (*N/A if not applicable*)	
C1.5 Other Relevant Information (N/A *if not applicable*)	
C1.6 Are All Original Controls in Place (N/A *if not applicable*)	☐ *Yes* ☐ *No*
If No Please Specify	

C2 - Root Cause Analysis and Follow-up

	Malicious Action	Process Failure	System Failure	Human Error
C2.1 Root Cause	☐ Abusive Content ☐ Web Defacement ☐ Malicious Code ☐ Virus	☐ Deficient Monitoring and Control ☐ Communication Issues ☐ Improper Operations ☐ Inadequate Change Management	☐ Hardware Failure ☐ Network Failure ☐ Database Issues ☐ Software / Application Failure	☐ Unintended ☐ Inaction ☐ Insufficient Resources ☐ Other (use space below)

- ☐ Worm
- ☐ Trojan
- ☐ Spyware
- ☐ Dialler
- ☐ Rootkit
- ☐ **Information Gathering**
- ☐ Scanning
- ☐ Sniffing
- ☐ Social Engineering
- ☐ **Intrusions**
- ☐ Privileged Account Compromise
- ☐ Unprivileged Account Compromise
- ☐ Application Compromise
- ☐ Bot
- ☐ **Availability**
- ☐ DOS
- ☐ DDOS
- ☐ **Deliberate Internal Actions**
- ☐ Sabotage
- ☐ Theft
- ☐ **Deliberate External Physical Damage**
- ☐ Sabotage
- ☐ Physical Attack of Premises
- ☐ **Information Content Security**
- ☐ Unauthorised Access to Information
- ☐ Unauthorised Modification of Information
- ☐ **Fraudulent Actions**
- ☐ Unauthorised Use of Resources
- ☐ Copyright
- ☐ Masquerade
- ☐ Phishing
- ☐ **Advanced Persistent Threat** (Please indicate number in space provided for Other)
- ☐ **Other** (use space below)

- ☐ **Inadequacy of Internal Procedures and Documentation**
- ☐ **Recovery Issues**
- ☐ **Other** (use space below)

- ☐ **Physical Damage**
- ☐ **Other** (use space below)

- ☐ **External Event**
- ☐ **Failure of supplier / technical service provider**
- ☐ **Force Majeure**
- ☐ **Other** (use space below)

- ☐ **Other** — Please specify *(please indicate whether Malicious Action, Process Failure, System Failure, Human Error, External Event, or Other)*
- ☐ **Still Under Investigation** (*Information to be provided in an another Report*)

C2.2 Other Relevant Information on the Root Cause	
C2.3 Main Corrective Actions/Measures Taken or Planned to Prevent the Incident from Happening again in the Future	

C3 - Additional Information

C3.1 Has the Incident Been Shared with other Licence Holders / Authorised Persons? (N/A if not applicable)	

C3.2 Has any Legal Action Been Taken Against the Licence Holder / Authorised Person? (N/A if not applicable)	
C3.3 Assessment of the Effectiveness of the Actions Taken	

Major ICT-Related Incident Report
A - Initial Report Explainer

A0.1 Report Date and Time	The date and time at which the Initial Report has been compiled.
A0.2 Incident Reference Number	A reference number is issued by the MFSA at the time of the initial report to unequivocally identify the incident. If this is known to the Licence Holder / Authorised Person (if, for instance, an Initial Report is being resent after the MFSA issued the reference number), it should be inputted. Please write N/A if not applicable.
A1 - General Details	
A1.1 Licence Holder / Authorised Person Name *(as per MFSA Financial Services Register)*	Full name of the Licence Holder / Authorised Person as it appears on the MFSA Financial Services Register.
A1.2 Licence Holder / Authorised Person Identification (*as per MFSA Financial Services Register*)	Identification of the Licence Holder / Authorised Person as it appears on the MFSA Financial Services Register.
A1.3 Company Registration Number (*MBR*)	Malta Business Registry Company Registration Number.
A1.4 Licenced/Authorised Activities Affected by the Incident	Select the financial services activities licenced/authorised by the Malta Financial Services Authority, which are affected by the Incident. If none of the listed financial services, please select "*Other* " and specify within the space provided.
A1.5 Head of Group (N/A *if not applicable*)	In case of groups please indicate the name of the head entity. Please write N/A if not applicable.
A1.6 Head of Group Country of Establishment (N/A *if not applicable*)	In case of groups please indicate the country of establishment of the head entity. Please write N/A if not applicable.
A1.7 Country/ies Affected by the Incident (select *where applicable*)	Please select the country or countries where the impact of the incident has materialised irrespective of the severity of the incident in the other country/countries. It may or may not be the same as the home Member State.
A1.8 Primary Contact Person	The name, surname, designation, email address, direct landline and mobile number (the details) of the person responsible for reporting the incident or, the details of the person in charge of the incident management/risk department or similar area, at the affected Licence Holder / Authorised Person.
A1.9 Secondary Contact Person	The details of an alternate person responsible for reporting the incident or, the details of the alternate person in charge of the incident management/risk department or similar area, at the affected Licence Holder / Authorised Person.
A2 - Incident Detection and Classification	
A2.1 Incident Detection Date and Time	Date and time at which the incident was first identified.
A2.2 Incident Classification Date and Time	Date and time at which the security or operational incident has been classified as major.
A2.3 Incident Detection Mechanism	Indicate whether the incident was detected by one of the detection mechanisms provided. If it was none of those, please provide an explanation in the corresponding field.
A2.4 Incident Type	Indicate whether, to the best of your knowledge and if the information is available, it is an operational or a security incident. **Operational**: incident stemming from inadequate or failed processes, people and systems or events of force majeure that affect the integrity, availability, confidentiality and/or authenticity of a financial service/s. **Security:** Unauthorised access, use, disclosure, disruption, modification or destruction of the Licence Holder / Authorised Person's assets that affects the integrity, availability, confidentiality and/or authenticity of a financial service/s. This may happen, among other things, when the Licence Holder / Authorised Person experiences a breach of security of network or information systems.
A2.5 Criteria for Classifying an ICT-Related Incident as Major	Please indicate which of the criteria have triggered the major incident report. Multiple choices may be selected between the criteria.
A2.6 A Short and General description of the Incident	Please explain briefly the most relevant issues of the incident, covering possible causes, immediate impacts, etc.

A2.7 Impact in other EU Member States (N/A if not applicable)	Please explain briefly the impact the incident had in another EU Member State. Please write N/A if not applicable.
A 2.8 Reporting to other Authorities	Please indicate whether the incident has been/will be reported to other authorities under separate incident reporting frameworks, if known at the time of reporting. If so, please specify the respective authorities.
A 2.9 Reasons for Late Submission (N/A if not applicable)	Please explain the reasons for requiring more than twenty-four hours to classify the Major ICT-Related Incident as Major.

Major ICT-Related Incident Report
B - Intermediate Report Explainer

B0.1 Report Date and Time	The date and time at which the Intermediate Report has been compiled.
B0.2 Incident Reference Number	The reference number issued by the MFSA at the time of the initial report to unequivocally identify the incident.

B1 - General Details	
B1.1 Changes Made in Sheet *A - Initial Report* (Question Numbers Only) (if more than one question, please separate each question number with a comma; *N/A if not applicable*)	Please indicate the question numbers within the Initial Report (related to the same incident) whereby any changes were made to the information already provided. Please write N/A if not applicable.
B1.2 Description of the Changes Made in *Sheet A - Initial Report* (*N/A if not applicable*)	Please indicate what changes were made within the Initial Report (related to the same incident) to the information already provided. Please write N/A if not applicable.
B1.3 What is/was the Specific Issue?	Please provide a more detailed description of the incident, by describing the main features.
B1.4 How did the Incident Start?	Please describe how the incident started.
B1.5 How did it Evolve?	Please describe how the incident evolved.
B1.6 Was it related to a previous incident?	Please indicate whether or not the incident is related to a previous incident or incidents, in case this information is available. If the incident has been related to previous incidents, please specify which ones.
B1.7 Were Other Licence Holders / Authorised Persons / Third Parties Affected or Involved?	Please indicate whether or not the incident has affected or involved other service providers/third parties. If the incident has affected or involved other service providers/third parties, please list them and provide more information.
B1.8 Incident Start Date and Time	Date and time at which the incident started.
B1.9 Has the Incident been Resolved?	Did you recover from the incident and restore your capabilities and/or services that were impaired due to the incident? If yes, please provide the date and time at which the incident has been resolved.
B2 - Incident Classification and Impact	

B2.1 Incident Classification

Licence Holders / Authorised Persons should indicate which thresholds are or will likely be reached by the incident, if any, and the related figures.

Licence Holders / Authorised Persons should provide concrete values for these variables, which may be either actual figures or estimations.

Number of transactions affected, **percentage of transactions affected** (if applicable) as part of the same financial services that have been affected by the incident and the total value of the transactions. As a general rule, Licence Holders / Authorised Persons should understand as 'transactions affected' all domestic and cross-border transactions that have been or will likely be directly or indirectly impacted by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the transaction message was altered, and those that were fraudulently ordered (have the funds been recovered or not). Furthermore, Licence Holders / Authorised Persons should understand the regular level of transactions to be the daily annual average of domestic and cross-border transactions carried out with the same services that have been affected by the incident, taking the previous year as the reference period for calculations. In case Licence Holders / Authorised Persons do not consider this figure to be representative (e.g. due to seasonality), they should use another more representative metric instead and convey to the MFSA the underlying rationale for this approach in the field 'Additional Comments'. In the cases where transactions in non-Euro currencies are affected by the incident, when calculating the thresholds and reporting the value of the transactions affected, Licence Holders / Authorised Persons should convert the amount of the transactions in non-Euro currency to Euro by using the ECB daily reference exchange rate for the day preceding the submission of the incident report.

Licence Holders / Authorised Persons should indicate which thresholds are or will likely be reached by the incident, if any, and the related figures:

Users affected: total number of users that have been impacted and percentage of users affected in relation to the total number of users. Licence Holders / Authorised Persons should understand as 'users affected' all customers (either domestic or from abroad, consumers or corporates) that have a contract with the affected Licence Holders / Authorised Persons that grants them access to the affected service, and that have suffered or will likely suffer the consequences of the incident. Authorised Persons / Licence Holders should recur to estimations based on past activity in order to determine the number of users that may have been using the service during the lifetime of the incident. In the case of Licence Holders / Authorised Persons offering operational services to others, that Licence Holder / Authorised Person should only consider its own users (if any), and the Licence Holder / Authorised Person receiving those operational services should also assess the incident in relation to their own users. Furthermore, Licence Holders / Authorised Persons should take as the total number of users the aggregated figure of domestic and cross-border users contractually bound with them at the time of the incident (or, alternatively, the most recent figure available) and with access to the affected service/s, regardless of their size or whether they are considered active or passive users.

Service Downtime: Licence Holders / Authorised Persons should consider the period of time that any task, process or channel related to the provision of services is or will likely be down and, thus, prevents i) the initiation and/or execution of a service and/or, ii) access to an account. Licence Holders / Authorised Persons should count the service downtime from the moment the downtime starts, and they should consider both the time intervals when they are open for business as required for the execution of services as well as the closing hours and maintenance periods, where relevant and applicable. If Licence Holders / Authorised Persons are unable to determine when the service downtime started, they should exceptionally count the service downtime from the moment the downtime is detected.

Breach of Security Measures: Licence Holders / Authorised Persons Holders should determine whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of services.

Economic Impact: Licence Holders / Authorised Persons should consider both the costs that can be connected to the incident directly and those which are indirectly related to the incident. Among other things, Licence Holders / Authorised Persons should take into account expropriated funds or assets, replacement costs of hardware or software, other forensic or remediation costs, fees due to non-compliance of contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, Licence Holders / Authorised Persons should only consider those that are already known or very likely to materialise. In the cases where the costs are in non-Euro currencies, when calculating the threshold and reporting the value of the economic impact, Licence Holders / Authorised Persons should convert the amount of the costs in non-Euro currency to Euro by using the ECB daily reference exchange rate for the day preceding the submission of the incident report.

Direct costs: amount of money (euro) directly caused by the incident, including those needed for the correction of the incident (e.g. expropriated funds or assets, replacement costs of hardware and software, fees due to non-compliance to contractual obligations).

Indirect costs: amount of money (euro) indirectly caused by the incident (e.g. customer redress/compensation costs, potential legal costs).

Geographical Spread: Licence Holders / Authorised Persons should consider the areas affected by the Major ICT-Related Incident, particularly if it affects up to **two (2) Member States** or More.

High Level of Internal Escalation: Licence Holders / Authorised Persons should consider whether, as a result of its impact on financial services, the management body as defined by EBA Guidelines on ICT and security risk management has been or will likely be informed about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. Furthermore, Licence Holders / Authorised Persons should consider whether, as a result of the impact of the incident a crisis mode has been or is likely to be triggered.

	Other Licence Holders / Authorised Persons / Financial Entities / Relevant Infrastructures Affected: Licence Holders / Authorised Persons should assess the impact of the incident on the financial services industry. In particular, Licence Holders / Authorised Persons should assess whether the incident has been or will likely be replicated at other Licence Holders / Authorised / Financial Entities / Relevant Infrastructures (not necessarily within the Maltese Jurisdiction), and whether it has affected / compromised or will likely affect / compromise the solidity of the financial system as a whole. Licence Holders / Authorised Persons should bear in mind various dimensions such as whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external or whether the Licence Holder / Authorised Person has stopped or will likely stop fulfilling its obligations in the financial services industry and any relevant infrastructure it forms part of. **Reputational Impact:** Licence Holders / Authorised Persons consider the level of visibility that, to their best knowledge, the incident has gained or will likely gain in the marketplace. In particular, Licence Holders / Authorised Persons should consider the likelihood of the incident to cause harm to the society as a good indicator of its potential to impact their reputation. Licence Holders / Authorised Persons should take into account whether i) service users and/or other Licence Holders / Authorised Persons have complained about the adverse impact of the incident, ii) the incident has impacted a visible financial service related process and is therefore likely to receive or has already received media coverage (considering not only traditional media, such as newspapers, but also blogs, social networks, etc. However, media coverage in this context means not only a few negative comments by followers, but there should be a valid report or a significant number of negative comments/alerts.), iii) contractual obligations have been or will likely be missed, resulting in the publication of legal actions towards the Licence Holder / Authorised Person, iv) regulatory requirements have not been complied with, resulting in the imposition of supervisory measures or sanctions that have been or will likely be made publicly available or v) similar type of incident has occurred before.
B2.2 Overall Impact	Please indicate which dimensions have been affected by the operational or security incident. Multiple choices may be selected. **Confidentiality:** the property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems. **Integrity:** the property of safeguarding the accuracy and completeness of assets (including data). **Availability:** the property of being accessible and usable on demand by an authorised entity.. **Authenticity:** the property of a source being what it claims to be.
B2.3 Financial Services Affected	Please provide details as to which financial services are affected by the incident.
B2.4 What are the Consequences? (in particular for users)	Please provide details as to the consequences, the affected financial services highlighted in question B2.3, have on the users of those financial services.
B3 - Incident Description	
B3.1 Incident Type	Indicate whether, it is an operational or a security incident. **Operational**: incident stemming from inadequate or failed processes, people and systems or events of force majeure that affect the integrity, availability, confidentiality and/or authenticity of a financial service/s. **Security:** Unauthorised access, use, disclosure, disruption, modification or destruction of the Licence Holder / Authorised Person's assets that affects the integrity, availability, confidentiality and/or authenticity of a financial service/s. This may happen, among other things, when the Licence Holder / Authorised Person experiences a breach of security of network or information systems.
B3.2 Root Cause	Please indicate what the root cause of the incident is or, if it is not known yet, the one that is the most likely. Multiple choices may be selected (please note that the root cause should be distinguished from the impact of the incident). Guidelines on how to fill this section are provided within the *Annex to Explainers* .
B3.3 Was the Incident Affecting you Directly, or Indirectly through a Service Provider	Please indicate whether or not the incident has targeted directly the Licence Holder / Authorised Person or affect it indirectly through a third party, in case this information is available. In case of an indirect impact, please provide the name of the service provider(s).
B4 - Incident Response and Mitigation	
B4.1 Which actions/measures have been taken so far or are planned to recover from the incident?	Please provide details about actions that have been taken or planned to be taken in order to temporarily address the incident.
B4.2 Was Crisis Management started (internal and/or external)?	Please indicate whether or not crisis management (internal and/or external) has started. If crisis management has started, please provide more information within the space available.
B4.3 Was the Incident communicated to the users?	Please indicate whether or not the incident was communicated to the users or any communication has taken place with any users. If yes, please provide more information within the space available.
B4.4 Has the Business Continuity Plan and/or Disaster Recovery Plan been activated?	Please indicate whether it has been the case and if so, provide the most relevant details of what happened (i.e. when they were activated and what it consisted of) within the space available.

C - Final Report Explainer

C0.1 Report Date and Time	The date and time at which the Final Report has been compiled.
C0.2 Incident Reference Number	The reference number issued by the MFSA at the time of the initial report to unequivocally identify the incident.
C0.3 Incident Re-classified back to Non-Major	If, following further evaluation, the Licence Holder / Authorised Person is re-classifying the incident back to non-major, the Licence Holder / Authorised Person is required to submit a Final Report, marking this question with a "Yes" and providing a reason within the space available.

C1 - General Details

C1.1 Changes Made in Sheet *A - Initial Report* (Question Numbers Only) (if more than one question, please separate each question number with a comma; *N/A if not applicable*)	Please indicate the question numbers within the Initial Report (related to the same incident) whereby any changes were made to the information already provided. Please write N/A if not applicable.
C1.2 Description of the Changes Made in *Sheet A - Initial Report* (*N/A if not applicable*)	Please indicate what changes were made within the Initial Report (related to the same incident) to the information already provided. Please write N/A if not applicable.
C1.3 Changes Made in Sheet *B - Intermediate Report* (Question Numbers Only) (if more than one question, please separate each question number with a comma; N/A if not applicable)	Please indicate the question numbers within the Intermediate Report (related to the same incident) whereby any changes were made to the information already provided. Please write N/A if not applicable.
C1.4 Description of the Changes Made in Sheet *B - Intermediate Report* (*N/A if not applicable*)	Please indicate what changes were made within the Intermediate Report (related to the same incident) to the information already provided. Please write N/A if not applicable.
C1.5 Other Relevant Information (N/A *if not applicable*)	Please provide any other relevant information. Please write N/A if not applicable.
C1.6 Are All Original Controls in Place (N/A *if not applicable*)	Please indicate whether or not the Licence Holder / Authorised Person had to cancel or weaken some controls at any time during the incident. If so, please indicate whether all controls are back in place and, if not, explain in the free text field which controls are not back in place and the additional period required for their restoration.

C2 - Root Cause Analysis and Follow-up

C2.1 Root Cause	Please indicate what the root cause of the incident is or, if it is not known yet, the one that is the most likely. Multiple choices may be selected (please note that the root cause should be distinguished from the impact of the incident). Guidelines on how to fill this section are provided within the *Annex to Explainers* .
C2.2 Other Relevant Information on the Root Cause	Please provide any additional details on the root cause, including the preliminary conclusions drawn from the root cause analysis.
C2.3 Main Corrective Actions/Measures Taken or Planned to Prevent the Incident from Happening again in the Future	Please, describe the main actions that have been taken or are planned to be taken in order to prevent a future reoccurrence of the incident.

C3 - Additional Information

C3.1 Has the Incident Been Shared with other Licence Holders / Authorised Persons? (N/A if not applicable)	Please provide an overview as to which other Licence Holders / Authorised Persons have been reached out, either formally or informally, to debrief them about the incident, providing details of the Licence Holders / Authorised Persons that have been informed, the information that has been shared and the underlying reasons for sharing this information. Please write N/A if not applicable.
C3.2 Has any Legal Action Been Taken Against the Licence Holder / Authorised Person? (N/A if not applicable)	Please, indicate whether, at the time of filling out the final report, the Licence Holder / Authorised Person has suffered any legal action (e.g. taken to court, lost the licence) as a result of the incident.
C3.3 Assessment of the Effectiveness of the Actions Taken	Please include, where available, a self-assessment of the effectiveness of the actions taken during the duration of the incident, including any lessons learnt from the incident.

Major ICT-Related Incident Report

Annex to Explainers

Table 1: Root Cause

Malicious action – External or internal actions intentionally targeting the Licence Holder / Authorised Person. These are separated into the following categories:

Abusive Content – e.g. web defacement.
Malicious code - e.g. such as a virus, worm, trojan, spyware.
Information gathering - e.g. scanning, sniffing, social engineering.
Intrusions - e.g. privileged account compromise, unprivileged account compromise, application compromise, bot.
Availability - an attempt to make an online service unavailable.
Deliberate internal actions – e.g. sabotage, theft.

Deliberate external physical damage - e.g. sabotage, physical attack of the premises/data centres.
Information content security - unauthorized access to information, unauthorized modification of information).
Fraudulent actions - unauthorized use of resources, copyright, masquerade, phishing.
Others (use space below) - the cause of the incident is none of the above. Further details should be provided in the free text field.

Process failure: the cause of the incident was a poor design or execution of a process, the process controls and/or the supporting processes (e.g. process for change/migration, testing, configuration, capacity, monitoring). These are separated into the following categories:

Deficient monitoring and control - e.g. in relation to running operations, certificate expiring dates, licence expiring dates, patch expiring dates, defined maximum counter values, database fill levels, user rights management, dual control principle.
Communication issues - e.g. between market participants or within the organisation.
Improper operations - e.g. no exchange of certificates, cache is full.
Inadequate change management - e.g. unidentified configuration errors, roll-out including updates, maintenance issues, unexpected errors.
Inadequacy of internal procedures and documentation - e.g. lack of transparency regarding functionalities, processes and occurrence of malfunctioning, absence of documentation.
Recovery issues - e.g. contingency management, inadequate redundancy.
Others (use space below) - the cause of the incident is none of the above. Further details should be provided in the free text field.

System failure: the cause of the incident is associated with a non-adequate design, execution, components, specifications, integration or complexity of the systems, networks, infrastructures and databases that support an activity. These are separated into the following categories:

Hardware failure – failure of physical technology equipment that runs the processes and/or stores the data needed by Licence Holders / Authorised Persons to carry out their activity/ies (e.g. failure of hard drives, data centres, other infrastructure).
Network failure – failure of telecommunications networks, either public or private, that allow the exchange of data and information (e.g. via the Internet) during a process.
Database issues – data structure which stores personal and transaction-related information needed to execute transactions.
Software/application failure – failures of programs, operating systems, etc. that support the provision of services by the Licence Holder / Authorised Person (e.g. malfunctions, unknown functions).
Physical damage – e.g. unintentional damage caused by inadequate conditions, construction work.
Other (use space below) - the cause of the incident is none of the above. Further details should be provided in the free text field.

Human error: the incident was caused by the unintentional mistake of a person, be it as part of a procedure (e.g. uploading a wrong file) or related with it somehow (e.g. the power is accidentally cut-off and the activity is put on hold). These are separated into the following categories:

Unintended - e.g. mistakes, errors, omissions, lack of experience and knowledge.
Inaction - e.g. due to lack of skills, knowledge, experience, awareness.
Insufficient resources - e.g. lack of human resources, availability of staff.
Other (use space below) - the cause of the incident is none of the above. Further details should be provided in the free text field.

External event: the cause is associated with events generally outside the organisation's control. These are separated into the following categories:

Failure of a supplier/technical service provider - e.g. power outage, internet outage, legal issues, business issues, service dependencies.
Force majeure - e.g. power failure, fires, natural causes such as earthquakes, floods, heavy precipitation, heavy wind.
Other (use space below) - the cause of the incident is none of the above. Further details should be provided in the free text field.

Other: the cause of the incident is none of the above. Further details should be provided in the free text field.