



Autoriti Monetari Brunei Darussalam
Major IT Incident Report Form

FI's Reference No:

Date:

Section 1 :	Details
FI Name:	
FI Sector Type:	
Reported By:	
Designation :	
Department:	
Telephone No.:	(O) (M)
E-mail :	
Section 2 :	Incident Analysis
Report Creation Date/Time:	
Incident Identification (Date/Time):	
Incident Location:	
Incident Type:	<input type="checkbox"/> Hardware <input type="checkbox"/> Software <input type="checkbox"/> Network <input type="checkbox"/> End-User <input type="checkbox"/> Infrastructure <input type="checkbox"/> Cybersecurity For Cybersecurity Incident, please specify the type: <input type="checkbox"/> DDOS/DOS <input type="checkbox"/> Ransomware <input type="checkbox"/> Data Breach <input type="checkbox"/> Virus outbreak <input type="checkbox"/> Website defacement <input type="checkbox"/> Unauthorised access <input type="checkbox"/> Insider breach <input type="checkbox"/> Other: _____
Impact:	<input type="checkbox"/> FIs core service <input type="checkbox"/> Related service <input type="checkbox"/> FIs website <input type="checkbox"/> Customer data <input type="checkbox"/> Stakeholder data <input type="checkbox"/> Employee data <input type="checkbox"/> ATM/Kiosk service <input type="checkbox"/> Smartphone apps <input type="checkbox"/> Social Media <input type="checkbox"/> Other: _____
Is this a new incident? <input type="checkbox"/> Yes <input type="checkbox"/> No If no, please provide reference to previous incident report:	
Section 3:	Summary of Incidents
Indicators (Root cause analysis):	
Measures and Actions Taken:	
Recommendations and Lesson learned:	
Restoration of Service Time:	
Resolution Time:	

How to fill in the form?

FI Name:	Name of the institution
FI Sector Type:	Type of license (e.g. Banking, Insurance Companies, Money Changer)
Reported By:	Name of the reporting person
Designation :	Job title of the reporting person
Department:	Department/Unit/Division of the reporting person
Telephone No.:	Mobile and/or office number
E-mail :	Official email address of the person
Report Creation Date/Time:	When is this report prepared?
Incident Identification (Date/Time):	When did the incident happen?
Incident Location:	Where did the incident happen?
Incident Type: <i>(you can tick more than one)</i>	<p>Type of Major Incidents</p> <ul style="list-style-type: none"> • Hardware: Major server, storage and device related issues • Software: Major system, software or application related issues • Network: Major network or internet issues • End-User: Major issues caused by business user's laptop or desktop • Infrastructure: Major issues related to power, building or the environment • Cybersecurity: <ul style="list-style-type: none"> ▪ DDOS/DOS (Distributed Denial of Service attack) ▪ Ransomware ▪ Data breach (e.g. data loss, data leak, stolen data) ▪ Virus outbreak (e.g. malware infection on more than 3 computers or directly on a critical server) ▪ Website defacement (unauthorised modification to website including social media page) ▪ Unauthorised access (hacking, intrusion or identity theft) ▪ Insider breach (sabotage, disgruntled employees or social engineering) ▪ Others: cyber fraud, cyber espionage or phishing
Impact: <i>(you can tick more than one)</i>	<p>What were impacted?</p> <ul style="list-style-type: none"> • FIs core service (e.g. business core system, front desk system) • Related service (any non-core system such as reward points service) • FIs website (company website or customer online portal) • Customer data (any customer data including transactions) • Stakeholder data (e.g. AMBD data, other FIs data, vendor data) • Employee data • ATM/Kiosk service • Smartphone apps • Social media • Other: financial, reputation, legal, compliance
Indicators (Root cause analysis):	
What cause the incidents? How did it happened?	
Measures and Actions Taken:	
What are the actions taken (in chronological order) and any measures to prevent further attack?	
Recommendations and Lesson learned:	
Next course of actions or improvements recommended to be performed (e.g. perform upgrade, review procedure) by the FI. Any useful information or advice that can be shared to AMBD and other FIs.	
Restoration of Service Time:	When is the service restored?
Resolution Time:	When is the incident verified as resolved?