MANAGEMENT OF IT INCIDENT

Prepared By:-	Approved By:-
	
Name : Ahmad Naim bin Hamat	Name : Nurmaliza binti Jumaat
Position : Senior Deputy Director Information Technology Division	Position : Director Information Technology Division
Date : 24/10/2025	Date : 24/10/2025

1.0 OBJECTIVE

This procedure aims to define the management of IT incidents within the IT service operations offered by the Information Technology Division. The management of IT incidents seeks to restore the IT service operations as quickly as possible after an unplanned disruption and to minimize the impact on academic, research, and administrative functions.

2.0 SCOPE

2.1 This procedure applies to all IT services and systems managed by the Information Technology Division, including user-reported issues, automated alerts, and vendor-managed platforms and services.

2.2 This procedure shall be implemented in accordance with IIUM's ICT Security Procedure in compliance with ISO/IEC 27001:2022 requirements to ensure confidentiality, availability, and integrity in all processes. All processes, decisions, and activities under this policy/guideline must uphold the principles of confidentiality, availability, and integrity to protect the information, data, and assets.

3.0 ACCOUNTABILITY

Incident Manager and Assistant Incident Manager

4.0 ABBREVIATION

4.1	Incident	:	An unplanned interruption or reduction in the quality of an IT service
4.2	Cyber Security Incident	:	A breach or threat that compromises the confidentiality, integrity, or availability of data or systems.
4.3	Major Incident	:	A high-impact incident that cause significant disruption to critical services based on Business Impact Assessment (BIA) and Priority Matrix.
4.4	i-First System	:	The central point of logging and tracking service requests and complaints from users.
4.5	SLA (Service Level Agreement)	:	Agreed timeframes for response and resolution.

4.6	OnTrack System	:	Logging system of major and high impact incidents, and cyber security incidents.
4.7	BIA	:	Business Impact Assessment

5.0 REFERENCE

5.1 IIUM ICT Policy
5.2 ICT Regulations
5.3 IIUM Information Management Policy
5.4 IIUM ICT Security Procedure
5.5 Anti-Bribery and Corruption Policy
5.6 IT Infrastructure Library (ITIL)
5.7 Control of Business IT (COBIT)
5.8 Procedure of IT Service Request

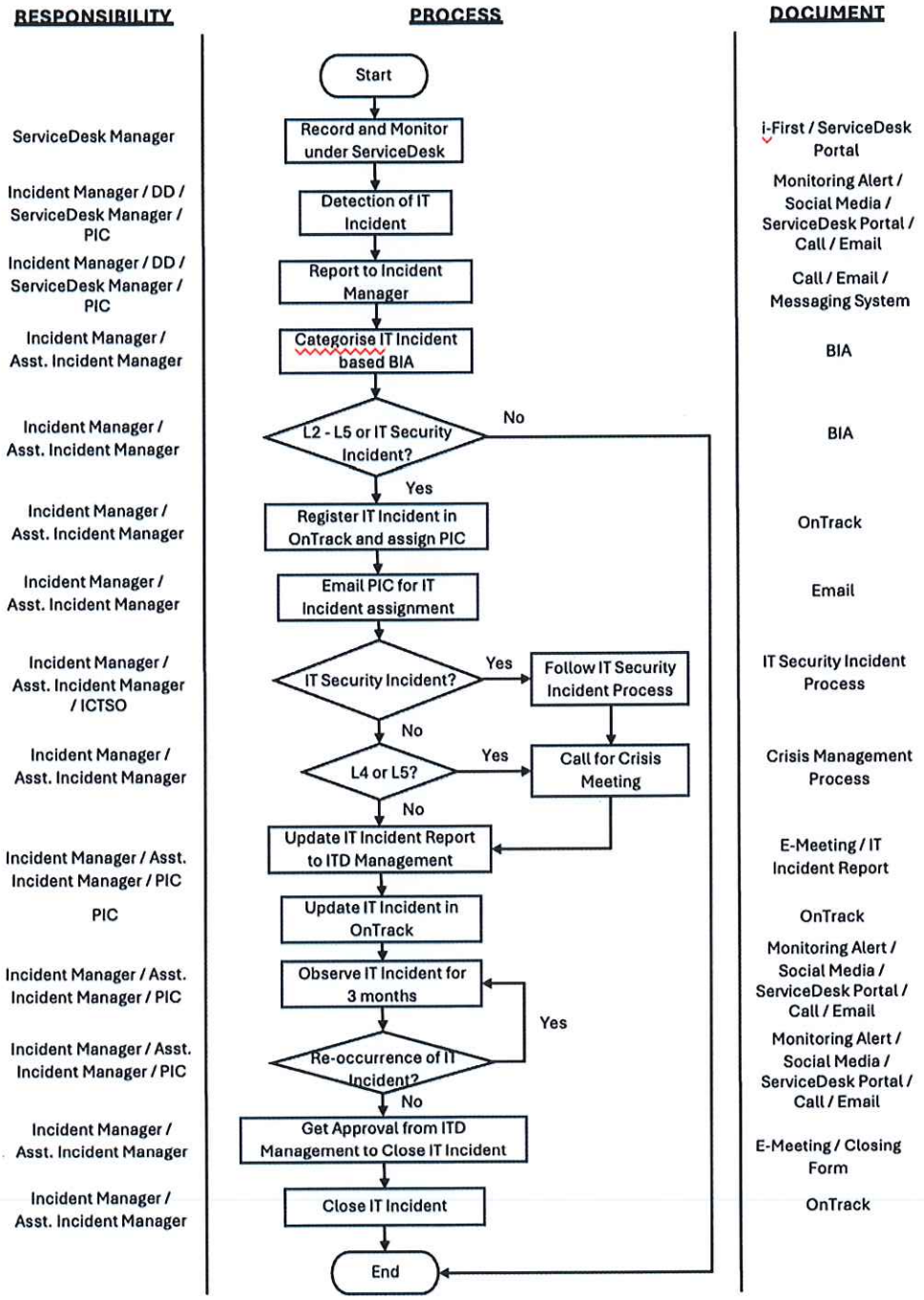
6.0 RECORD RETENTION PERIOD

No.	Quality Records	Location	Retention Period	Responsibility
1	IT Incident Record	OnTrack	3 years	Incident Manager Assistant Incident Manager PIC
2	IT Service Desk Record	i-First System	3 years	Service Desk Manager PIC

7.0 RESPONSIBILITY AND DETAILED PROCEDURE

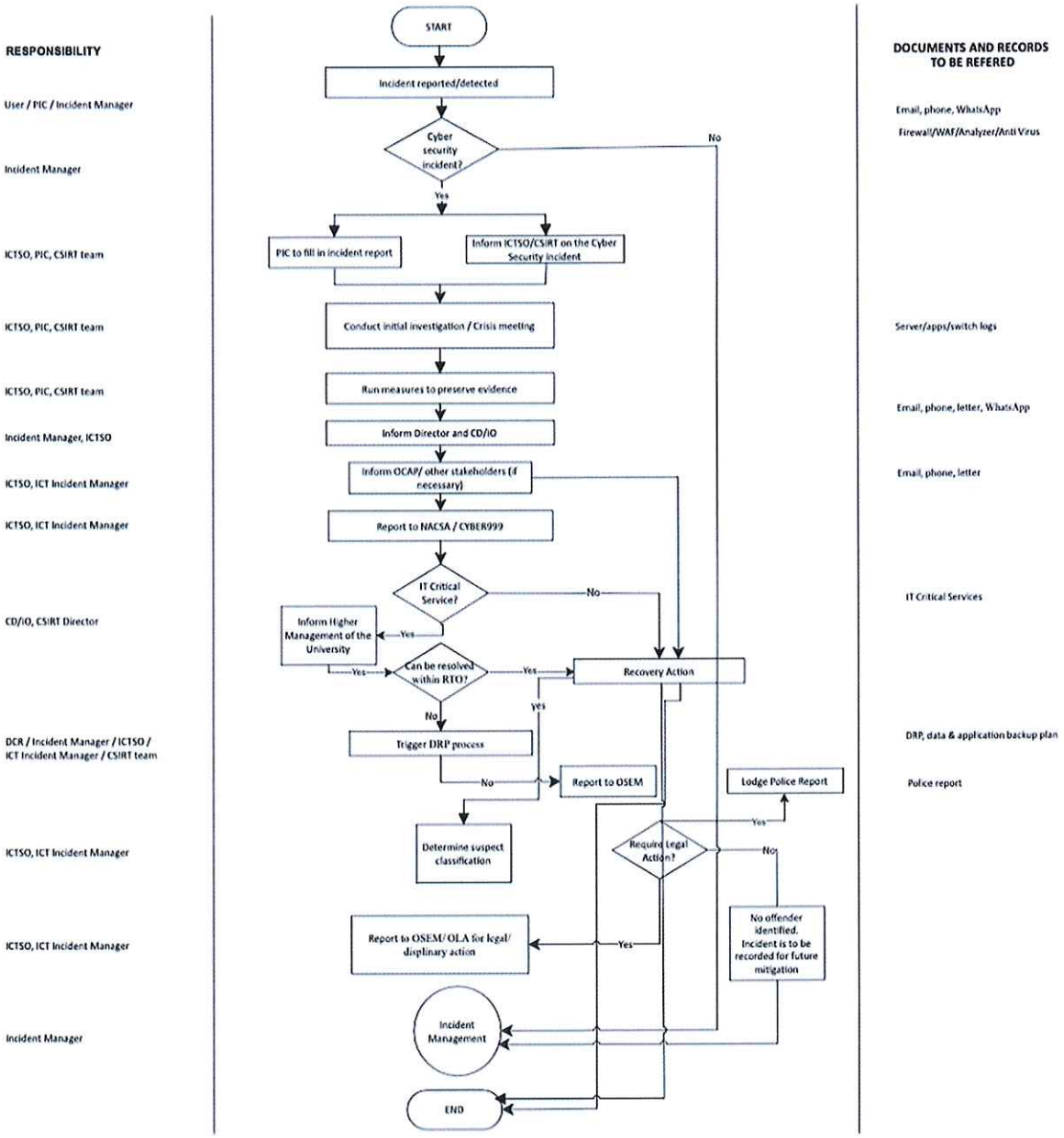
7.1 Flowchart

FLOWCHART ON THE MANAGEMENT OF IT INCIDENT



Version: 0.1
Revision: 1
Effective Date 01/08/2025

CYBER SECURITY INCIDENT WORKFLOW



7.2 Roles and Responsibilities

Roles	Responsibility
IT Services Help Desk	Logs, categorizes, prioritizes, and provides first-lines support.
Incident Manager	Coordinates response, ensures SLAs are met, handles major incidents.
ICTSO / ICT Security Incident Manager	Oversees and investigates cyber security incidents, leads response.
IT Support / Resolver Team	Diagnose and resolve technical issues.
PIC	IT Officers / Engineers leading the resolution of an IT Incident
Users	Report issues and cooperate with investigations.
Compliance / Legal	Provide support for data breaches and legal/regulatory reporting.

7.3 Incident Management Process

Step	Activity	Details

1	**Identification & Logging**	• Users or systems report incidents via:
		  o Helpdesk portal, email, phone, monitoring tools
		• Incidents classified as **cyber security-related** if they involve:
		  o Unauthorized access/Defacement
		  o Data leakage or exposure
		  o Malware/ransomware
		  o Phishing
		  o Suspicious behaviour

2	**Categorization**	• Categorize as:
		  o **IT Service Incident**
		  o **Cyber Security Incident**
		• Further subcategorize for reporting and triage (e.g., i-taleem failure, email spoofing)

3	**Prioritization**	• Based on **IIUM Business Impact Analysis (BIA)**
		• Cyber Security incidents are auto-escalated if they:
		  o Affect sensitive systems/data
		  o Are part of a targeted attack or malware outbreak
		• Use priorities (L1–L5) based on Business Impact Assessment (BIA); L5 for major or high-risk incidents

4	**Initial Diagnosis**	• PIC attempts resolution or containment (e.g., password reset, isolate device)
		• For cyber security incidents:
		  o **Immediately inform Cyber Security Officer**
		  o Contain impact (e.g., revoke access, block IP)

5	**Escalation**	**Functional**: Forward to relevant resolver or security team • **Hierarchical**: Notify IT management, legal, or institutional leadership as needed • For **data breaches**, follow legal and regulatory escalation protocols
6	**Investigation & Resolution**	• PIC / Incident Handler performs troubleshooting, ie. analyze logs, traffic, behaviour, etc. • Document actions and decisions • Apply fixes (technical or procedural) • If external systems/vendors are involved, initiate third-party coordination

7	**Communication**	• Notify affected users and stakeholders
		• For major or cyber security incidents:
		  o Use official university channels (email, web)
		  o Coordinate messaging with communications and legal teams if public impact is possible

8	**Closure**	Confirm issue resolution with user or system • Ensure logs, evidence, and RCA details are properly stored • Mark as **Security Closed** or **IT Incident Closed** with resolution details

7.4 Major Incident Handling

Step	Activity	Details
1	**Notify Incident Manager and Stakeholders**	Immediate alert to Incident Manager, ITD Management, and impacted service owners
2	**Launch Crisis Meeting**	Set up coordination meeting with technical teams, vendors, and stakeholders immediately.
3	**Assign Dedicated Resources**	Allocate a dedicated team to focus solely on resolution of the major incident
4	**Provide Frequent Updates**	**PIC / Incident Handler attempts resolution or containment** Status updates every **30–60 minutes** via bridge call, chat, or email
5	**Conduct Post-Incident Review**	Complete a **Post-Incident Review (PIR)** within **3 business days** to analyse cause, response, and improvements

7.5 Business Impact Analysis (BIA) – IIUM Severity Criteria

Level / Score	Matrix	Impact Descriptions										
		Governance	Financial	Financial - Quantitative Impact I	Financial - Quantitative Impact II	Reputation - Quantitative Impact	Legal / Non-compliance	Safety I	safety II	safety III	operational impact	Operational
1	1 - Insignificant	Little impact to governance	100% budget utilization	<10% financial loss	Financial impact to individual	IIUM image tarnished at individual level	No legal impact / no non-compliance	No injury - physically	No injury - psychologically	Safety impact to individual	Disruption of operation at personal level	No disruption of critical operation or services
2	2 - Minor	Some impact to governance	Some financial loss	10% - <20% financial loss	Financial impact to agency	IIUM image tarnished at agencies level	Non-compliance requires opportunity for improvement	Minor injury - physically	Minor injury - psychologically	Safety impact to a group of people	Disruption of operation at agencies level	Up to 2 hour disruption
3	3 - Moderate	Moderate impact to governance	Significant financial loss	20% - <30% financial loss	Financial impact to campus	IIUM image tarnished at regional/campus level	Non-compliance that requires rectification	Major injury - physically	Major injury - psychologically	Safety impact to campus	Disruption of operation at regional / campus level	6 hours disruption
4	4 - High	Major impact governance	Major financial loss	30% - <40% financial loss	Financial impact to university	IIUM image tarnished at national/ university level	Non-compliance which leads penalised / legal action	Permanent disability - physically	Permanent disability - psychologically	Safety impact to university	Disruption of operation at national / university level	24 hours disruption
5	5 - Extremely High	Significant impact to governance	Huge financial loss	>= 40% financial loss	Financial impact to the country	IIUM image tarnished at International level	Non-compliance leading to termination of operation	Death - physically	Attempted / Successful suicide	Safety impact to national	Disruption of operation at International level	More than 24 hours disruption

7.6 Post-Incident Activities

Step	Activity	Details
1	**Conduct Root Cause Analysis (RCA)**	• Mandatory for the following incidents: - P1 (Major) - Repeated maximum three (3) times - Cyber Security-related • Identify not just technical root causes, but also contributing process or human factors. • Document findings in an RCA report and share with stakeholders. • Include recommendations for prevention and mitigation.
2	**Update Knowledge Base at iStack**	• Create or update internal knowledge articles for support teams. • Include detailed description of symptoms, diagnosis steps, resolution, and lessons learned. • Tag articles appropriately (e.g., service name, incident type) for easy search. • Ensure access controls are applied if the information is security-sensitive.
3	**Link to Problem Records at OnTrack**	• If incident recurrence more than three (3) times, escalate to **Problem Management**. • Create a **Problem Record** to initiate long-term analysis and corrective action. • Assign ownership and track progress through Problem Management workflow. • Monitor related incidents until root cause is addressed or permanently resolved.