AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

The purpose of this document is to outline the procedures and responsibilities for ensuring continuity and timely recovery of our IT observability and security management solutions in the event of any disruption or disaster.

SCOPE

This control applies to all systems, applications, cloud infrastructure, and IT services owned or utilized by the company in the delivery of our IT observability and security management solutions. It includes cloud-hosted services, development environments, customer-facing services, and remote collaboration platforms essential for operations.

REFERENCE

ISO/IEC 27001 Standard	Annex A 5.29 Information security during disruption Annex A 5.30 ICT readiness for business continuity Annex A 8.14 Redundancy of information processing facilities

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this procedure.

The Incident Response Team (IRT) as per *ISMS-ORG-10 Information Security Event & Incident Management* shall provide advice on information security continuity options, invoke the established business continuity plans (BCPs) and initiate recovery efforts.

The following roles will have critical responsibilities during disruptive incidents leading to damage of critical information and communication technology (ICT) infrastructure, systems and networks.

1. **Top Management**– Strategic decisions on relocation, vendor engagement, and recovery funding.
2. **Finance Team** – Ensures financial readiness for both small-scale and major recovery needs.
3. **Technical Team** – Manages application and infrastructure recovery, tests redeployments, and performs system impact assessments.
4. **System Admin** – Validates system and cloud service performance, applies patches/fixes, and coordinates restoration from backup
5. **Functional Representatives (e.g., Department Heads)** – Coordinates recovery tasks within their functional areas and ensures local continuity of operations.

External contact list for ICT suppliers is maintained in *ISMS-ORG-03-F2 Authorities and Special Interest Group Contact List.*

PROCEDURE

A. Minimum Business Continuity Objective (MBCO), Recovery Time Objective (RTO), and Recovery Point Objective (RPO)

Our organisation MBCO, RTO and RPO for our provision of IT observability and security management solutions are as follows:

Objectives	Description	Targets
MBCO	The minimum acceptable level of service your customers must have during a disruption	Maintain partial monitoring visibility during disruptions (e.g., degraded UI or slower refresh rate), but core alerting and API access must resume within 4 hours.
RTO	Maximum tolerable downtime before full recovery must be completed	4 to 8 hours, with a target of <4 hours for customer-facing features (e.g., alerting, dashboards, APIs).
RPO	Maximum tolerable data loss (e.g., metrics, logs, events)	15 minutes for critical security events, 1 hour for logs and general observability data

B. Impact Tolerance

The below table defines the levels for the types of loss the organisation cannot sustain.

Impact Type	**Unacceptable Impact**
Financial	>50% drop in annual revenue
Reputation	Major loss of trust, regulatory inquiry, or widespread customer dissatisfaction
Operations	Loss of key enterprise customer(s)
Human	Serious injury or fatalities (if co-working site is involved)
Legal / Regulatory	Regulatory action that halts service delivery or results in major penalties

C. Continuity Scenarios

Based on our business-critical product/service in the preceding sections, the following continuity scenarios have been identified as the basis for our business continuity and disaster recovery plan.

Scenario	**Description**	**Impact on Business-Critical Product/Service**	**Mitigation in Place**
Loss of office access	Fire, pandemic lockdown, or power outage affecting shared office	Negligible – remote-first operations, no dependency on physical location	• Employees work remotely using company-issued laptops • All systems hosted in the cloud with remote access

			• Shared office has building-managed fire safety and backup power systems • Remote operations support continued access to systems, ensuring MBCO is met
Loss of network connectivity	ISP issues or outage in shared office	Low – platform is cloud-hosted; staff can continue operations using alternatives	• Employees use mobile hotspots or home broadband • Remote-friendly tools ensure collaboration continuity • Monitoring and alerting systems remain functional with no dependence on office LAN • Core services operate independently of office connectivity, aligning with RTO
Loss of access to critical IT systems	Cloud infrastructure outage, major misconfiguration, or cyberattack	High – impacts core observability and monitoring functions	• Multi-zone and multi-region redundancy in cloud for high availability • Real-time data replication and automated recovery scripts support 15min–1h RPO • Auto-scaling and failover mechanisms to restore degraded functionality within <4h • CI/CD and Infrastructure-as-Code support full redeployment within RTO window
Widespread loss of staff	Mass illness, resignation wave, or team unavailability	Moderate – may delay manual interventions or support escalations	• Cross-training • Temporary contractors or outsourced partners for short-term recovery support • Essential operational knowledge maintained • Prioritization of critical customer-facing features during limited staff scenarios to meet MBCO and RTO targets

D. Remote Work and Alternate Site Schedule

- No dedicated standby office site is required.
- All staff are enabled to work remotely using laptops and secure access (MFA, VPN).
- Essential services are cloud-based and accessible from anywhere.

E. IT Service Continuity and System Backup

The following provides a breakdown of our essential IT systems, applications and services:

No.	System/ application	How is it hosted?	Where is the backup?	Backup Frequency	RPO	RTO
1	SaaS Platform	AWS multi-AZ	AWS (multi-AZ, cross-region for critical data)	Real-time replication + hourly snapshots	<15 min (critical events), <1 hr (other data)	<4 hours (goal), max 8 hrs
2	Microsoft 365	Microsoft Cloud	Microsoft-native backup & retention systems	Continuous	~0	<10 minutes
3	GitHub Repositories	GitHub Cloud	GitHub backup repos + internal cold storage	Real-time mirroring + daily exports	<1 hour	<2 hours
4	Security Event Logs	Cloud-native (SIEM)	Cloud backup w/ cold storage and event redundancy	Real-time ingestion and daily archive	<15 minutes	<2 hours

F. Redundancy Strategies

The company implements the following redundancy and recovery strategies to meet availability requirements and ensure ICT readiness for business continuity.

- Multi-zone cloud infrastructure for all production services
- Real-time data replication for critical systems
- Mobile internet fallback for employee access
- Cloud-native collaboration and code platforms

G. Business Impact Analysis and Recovery Playbooks

Scenario-based response guides are maintained as follows:

Scenario 1: Loss of Office Access Business Impact: Minimal operational disruption due to remote-first model; No dependency on shared physical infrastructure

Business-Critical Product/Service Impact: No impact to monitoring platform uptime; No compromise to core services or support	
Recovery Playbook	
Step	Action
Trigger	Office becomes inaccessible or unusable (fire, lockdown, blackout)
Initial Response	Notify staff; initiate remote work protocol
Continuity Activation	Enable full remote access; communicate via collaboration tools
System Access	Staff use laptops; VPN/MFA maintained
Recovery	Ensure 100% access to cloud systems; monitor for productivity disruption
Post-Recovery Review	Assess damage (if any), update asset inventory, validate employee readiness

Scenario 2: Loss of Network Connectivity Business Impact: Temporary communication delays; Minimal to no disruption for core operations Business-Critical Product/Service Impact: No platform downtime; Internal collaboration may be delayed without redundant access	
Recovery Playbook	
Step	Action
Trigger	Loss of office LAN or ISP connectivity
Initial Response	Notify affected users; instruct switch to mobile hotspots or home networks
Continuity Activation	Ensure continued use of cloud services via redundant connections
System Access	Critical systems remain cloud-hosted; access unaffected
Recovery	Maintain full operational continuity with degraded internal comms
Post-Recovery Review	In a shared office, not managing the office network; May consider alternate arrangements, if recurring

Scenario 3: Loss of Access to Critical IT Systems Business Impact: Major impact on observability, alerting, and client-facing services; Risk of SLA breach if unresolved within RTO Business-Critical Product/Service Impact: Degraded or unavailable platform features; Data loss risk if RPO thresholds are exceeded	
Recovery Playbook	
Step	Action
Trigger	Monitoring platform outage, critical service failures, security incidents
Initial Response	Engage IRT (per ISMS-ORG-10); assess scope, initiate impact containment
Continuity Activation	Activate failover procedures; switch to standby zones or regions
System Access	CI/CD used to redeploy infrastructure; automated health checks engaged
Recovery	Restore core alerting and APIs within <4h; logs/events restored to <15min–1h RPO
Post-Recovery Review	Conduct root cause analysis (RCA), patching, reporting to stakeholders

Scenario 4: Widespread Loss of Staff

Business Impact: Slower incident response and manual recovery processes; Delays in roadmap execution and support response Business-Critical Product/Service Impact: Potential RTO delays without automation or backup resources; Risks around manual recovery or investigation	
Recovery Playbook	
Step	Action
Trigger	Sudden reduction in available workforce (e.g., illness, attrition)
Initial Response	Assess available workforce capacity; reprioritize operational tasks
Continuity Activation	Activate cross-trained backup staff; engage contractors/outsourcing where applicable
System Access	Ensure unaffected staff have appropriate system access
Recovery	Focus on MBCO-first tasks (core alerting, platform stability)
Post-Recovery Review	Review staffing levels, succession planning, update SOPs and knowledge base

H. Testing

Testing must be conducted annually to ensure that all elements of the business continuity and disaster recovery plan are feasible, compatible, and effective.

A necessary objective of the test is to minimize interference and interruption of normal operations, while providing a thorough assessment of the planned capabilities to respond to disaster.

Test plan and a post-test report shall be documented and maintained by the ISMS MR.

FORMS

ISMS-ORG-11-F1 Exercise & Test Plan
ISMS-ORG-11-F2 Exercise & Test Report