IOIPG Malaysia REIT
Management

IOIPG REIT MANAGEMENT SDN BHD
Company Registration No. 202501026083 (1627496-A)
(Incorporated in Malaysia)

BUSINESS CONTINUITY MANAGEMENT POLICY

CONTENTS

1. INTRODUCTION 3
2. KEY ROLES AND RESPONSIBILITIES 3
3. BCM KEY COMPONENTS 4
4. EMERGENCY RESPONSE PROCEDURES 5
5. BCM FRAMEWORK AND POLICY MAINTENANCE 5

1. INTRODUCTION

IOIPG REIT Management Sdn Bhd ("Manager"), in its capacity as the Manager of IOIPG Malaysia Real Estate Investment Trust ("IOIPG REIT"), is the responsible entity of IOIPG REIT.

The purpose of this Business Continuity Management Policy ("Policy") is to outline the key principles and guidance for implementing and maintaining a Business Continuity Management ("BCM") framework for the Manager.

This Policy is supported by an internal Business Continuity Plan ("BCP") which sets out the procedures, recovery strategies, and critical system dependencies required to ensure that business operations can respond effectively to unexpected disruptions or adverse incidents.

The BCM framework is designed to ensure:

- Continuity of critical functions during a disruptive incident;
- Protection of tenant, hotel guest, employee, and unitholder interests;
- Minimisation of operational, financial, and reputational impacts; and
- Compliance with regulatory requirements

This Policy applies to all locations and employees of the Manager. It extends to core functions of the Manager, including investment, retail leasing, finance, compliance, and IT, as well as property-level operations managed in coordination with outsourced property and facility managers.

Critical vendors, outsourced functions, and information systems including but not limited to application software deployed at retail mall, the organisation's Enterprise Resource Planning systems and equivalent platforms, as well as other essential technology services such as finance software, email, and data storage) are also within the scope of the BCM framework.

2. KEY ROLES AND RESPONSIBILITIES

Key roles and responsibilities include:

Role	Responsibilities
Board of Directors ("Board")	• Approves the BCM policy, framework, and BCP. • Provides overall oversight of crisis management and recovery planning. • Provides strategic guidance during crisis management.
Risk and Sustainability Committee ("RSC")	• Sets the BCM policy, framework, and strategy, ensuring they are integrated into the Manager's enterprise risk management system. • Oversees the implementation of risk mitigation actions. • Reviews the continuity plans periodically to reflect changes in the business environment or technology, as well as reviewing the lessons learned.
Chief Executive Officer	• Leads the implementation of the BCM framework and BCP. • Ensures adequate resources are allocated for BCM activities. • Reviews updates to the BCM, BCP and crisis management plan. • Makes key management decisions during major disruptions and escalates to the RSC or the Board, where necessary.

Role	Responsibilities
Head of Legal and Compliance	• Provides reports to the Chief Executive Officer and the RSC on BCM and BCP testing, risk assessments, and recommended improvement actions. • Ensures compliance with legal and regulatory requirements, as well as contractual requirements related to business continuity and operational resilience. • Acts as the central liaison during disruption response and ensures communication across departments.
Heads of Department	• Develops and maintains department-specific operational continuity procedures. • Ensures staff are well trained and prepared for activation of BCP. • Identifies critical business functions and recovery priorities within their departments. • Coordinates development, maintenance, and documentation of BCM and BCPs. • Coordinates verification, review and testing and of BCM and BCP of critical outsourced service providers. • Organises drills, training, and simulation exercises relating to their respective departments. • Escalates significant risk exposures, control weaknesses, governance issues, or instances arising from or relating to any BCM and BCP to the Head of Legal and Compliance.
IT Officer	• Maintains IT recovery policies, including system backups, data restoration, and cybersecurity measures. • Oversees the IT Disaster Recovery Plan (DRP). • Ensures secure remote access, redundancy, and resilience of critical systems.
Critical Service Providers	• Maintains their own BCPs and DRPs aligned to the Manager's BCM framework. • Provides annual declarations of BCP and DRP readiness. • Complies with contractual requirements including reporting obligations, RTOs, and escalation triggers.
Employees	• Complies with BCM procedures and actively participates in training and simulation exercises. • Reports promptly incidents, and provides support for continuity and recovery efforts, as required. • Adheres to established communication and safety protocols during operational disruptions.

3. BCM KEY COMPONENTS

Key components of the BCM framework include:

Key Component	Description
Risk Assessment (RA)	• Identification of potential threats, including fire, flood, pandemic, cyberattack, public relations crisis, financial shocks, and other operational disruptions. • Risks shall be reviewed periodically and reflected in the risk register.
Business Impact Analysis (BIA)	• Evaluates functions' criticality, downtime tolerance, and potential operational, financial, regulatory, and reputational consequences. • Differentiates between essential and non-essential functions to prioritise recovery.

Key Component	Description
Critical Business Functions (CBF)	• Core activities such as tenancy management, rental billing, payroll, and regulatory filings must be prioritised for restoration. • Functions shall be categorised by level of criticality and mapped to recovery strategies.
Maximum Tolerable Downtime (MTD)	• Defines the threshold beyond which the Manager would suffer material damage or irrecoverable loss. • Specific MTDs will be set for each CBF and reviewed annually.
Recovery Time Objective (RTO)	• Establishes target recovery times for critical business functions (for example, payroll processing within 24 hours).
Recovery Procedures	• Defines strategies to maintain operations such as physical facilities restoration, alternate sites, remote work arrangements, backup systems, outsourcing and may include activation of contingency funds. • Includes, but is not limited to, the use of secure VPN access, off-site/cloud backups, redundant systems, and training requirements.
IT Recovery & Disaster Recovery Plan (DRP)	• Focuses on data restoration, system resilience, and continuity of core system and applications. • IT vendor and outsourced service provider coordination to recover financial systems, tenant management systems, back-up data and any other IT infrastructure and data. • Ensures cybersecurity safeguards (firewalls, encryption, monitoring) remain active during and after incidents.
Vendor & Service Provider Continuity	• Critical outsourced providers must maintain BCP and DRP capabilities. • Annual review of their BCP and DRP readiness is mandatory. • Service Level Agreements or the relevant engagement letters must include terms entailing reporting obligations, escalation triggers, and minimum continuity standards.
Personnel Safety & Security	• The safety and security of all persons is the paramount consideration during any disruption. • Evacuation procedures, first aid arrangements, and emergency contact lists shall be maintained, among others.
Crisis Communication Plan	• Predefined communication procedures and templates for staff, regulators, unitholders, and external stakeholders during and after a disruption. • This includes escalation to key management personnel and the RSC and the Board.

4. EMERGENCY RESPONSE PROCEDURES

Effective emergency response ensures that the immediate impact of any disruption is contained, personnel safety is prioritised, and critical stakeholders are notified without delay.

The Manager shall maintain clear emergency procedures that enable swift action, structured communication, and effective coordination with regulators, property managers, and service providers.

5. BCM FRAMEWORK AND POLICY MAINTENANCE

Business continuity planning is a dynamic process that must evolve alongside the Manager's operations, systems, and external risk landscape. Regular testing, updates, and training are essential to ensure the BCM framework remains effective and relevant. Maintenance activities ensure preparedness is not only documented but also embedded in in day-to-day practices across all business functions and properties.

This includes but not limited to, the following:

Activity	Description
Regular Testing	• Crisis drills, tabletop simulations, and IT recovery (i.e. IT DRP) shall be conducted annually or at such other intervals may be prescribed period by the Board. • Testing scenarios will cover both property-level disruptions (e.g. mall/hotel/office evacuation) and corporate-level events (e.g. IT/data outage).
Periodic Review and Updates	• BCM, BCP and DRP shall be reviewed annually, or sooner if triggered by material, operational, or environmental changes (e.g. pandemics, cyberattacks, regulatory updates). • Preventive controls for business continuity and cybersecurity risks are included in the Manager's Risk Register and periodically reviewed and updated.
Continuous Training	• Staff onboarding and refresher programmes shall include BCM awareness and role-specific responsibilities. • Heads of Department shall provide periodic trainings and shall ensure employees understand recovery procedures and escalation protocols.
Independent Audit	• Internal audit shall review the BCM at least once every three (3) years, or as and when required by the Audit Committee. • Findings and recommendations will be reported to the Board/Board Audit and Risk Committee.
Vendor BCM Alignment	• Critical outsourced service providers must demonstrate annual BCM readiness through declarations or certifications. • The IT Officer and the Heads of Department should ensure appropriate review of BCM and BCP of the critical outsourced service providers.

This Policy, together with all supplementary policies and procedures, shall be treated as a living document and will be reviewed at least annually, or earlier where necessary, to ensure that it continues to reflect evolving business needs, regulatory requirements, industry best practices, and any material changes in applicable laws, regulations, or the Manager's business operations.