IOIPG Malaysia REIT
Management

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

TECHNOLOGY MANAGEMENT POLICY

CONTENTS

1. INTRODUCTION 3
2. ROLES AND RESPONSIBILITIES 3
3. ACCESS CONTROL MANAGEMENT 4
4. DESKTOP, MOBILE COMPUTING DEVICE & STORAGE DEVICE USAGE 5
5. BACKUP, RESTORATION AND RESTORATION TESTING 6
6. CYBERSECURITY RISK MONITORING 7
7. CYBERSECURITY ESCALATION 7
8. IT OUTSOURCING 7
9. TECHNOLOGY PROJECT MANAGEMENT 7
10. SYSTEM ACQUISITION AND DEVELOPMENT 8
11. SYSTEM TESTING AND ACCEPTANCE 8
12. REVIEW AND AUDIT OF IT, TECHNOLOGY AND CYBERSECURITY 8
13. IT DISASTER RECOVERY PROCEDURES 9
14. TRAINING AND AWARENESS 9
15. POLICY MAINTENANCE 10

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 Manager is committed to ensuring that all information technology ("IT") systems, digital infrastructure, and data supporting IOIPG REIT's operations are managed securely, reliably, and in compliance with applicable laws and regulatory expectations.

This Technology Management Policy ("Policy") forms part of the Manager's broader governance and risk management framework. It provides the foundation for protecting information assets, preventing unauthorised access, strengthening resilience against cyber and technology risks, and ensuring operational continuity.

This Policy sets out minimum principles and requirements, which will be supplemented by detailed procedures and guidelines. These procedures will, at a minimum, align with the Securities Commission Malaysia's ("SC") Guidelines on Technology Risk Management ("Guidelines").

2. ROLES AND RESPONSIBILITIES

The effective implementation of this Policy requires clear accountability, defined responsibilities and coordinated efforts across all levels of governance within the Manager.

Each party across all levels and functions in the Manager plays a distinct yet complementary role in safeguarding information assets, mitigating technology-related risks, and ensuring that technology practices remain compliant with applicable regulatory requirements and industry standards.

The following table sets out the key roles and responsibilities within the Manager's IT governance framework:

Role	Key Responsibilities
Board of Directors ("Board")	• Provides overall oversight of IT and technology risks. • Approves key policies, disaster recovery plans, and material outsourcing/vendor contracts. • Ensures adequate resources are allocated for technology risk management. • Reviews audit findings and cyber incident escalations.
Risk & Sustainability Committee ("RSC")	• Monitors technology risk exposures, cybersecurity incidents, and regulatory compliance. • Reviews independent IT audit reports and remediation progress. • Ensures alignment with the Manager's broader risk appetite and governance framework on IT and technology risks.
Chief Executive Officer ("CEO")	• Implements IT and cybersecurity policies across the organisation. • Manages IT outsourcing arrangements, ensuring vendor performance and independence safeguards. • Allocates adequate resources and staffing to support IT resilience and cyber risk management. • Escalates material breaches, incidents, or risks to the RSC and the Board.

Role	Key Responsibilities
Principal person responsible for IT compliance function ("Responsible Person")	• Oversees overall IT functions including all day-to-day implementation and oversight of IT systems and computer hardware, IT risks and framework which include technology risk management, technology operations management, technology service provider management, cybersecurity management, etc. • Ensures adherence to the Guidelines, the Policy and other applicable regulatory requirements. • Maintains incident reporting protocols for cyber and technology-related matters. • Coordinates with system or data owners on IT monitoring and compliance oversight including monitoring of the IT service providers appointed for IOIPG REIT. • Reports material breaches to the CEO and the Head of Legal and Compliance of the Manager.

3. ACCESS CONTROL MANAGEMENT

The Manager is committed to maintaining secure access control over all information systems and data to prevent unauthorised use, protect sensitive information, and ensure accountability.

a) User Access Governance

- All access rights must be approved by authorised personnel (e.g. key management personnel) of the Manager;
- Access must be granted based on the principle of "least privilege", ensuring users only have the minimum level of access required to perform their roles.
- A user access register shall be maintained, documenting roles, approvals, and duration of access.
- Temporary/contractor access and access by outsourced IT functions must be time-bound and automatically revoked upon project completion or contract termination.

b) Password and Authentication Controls

All users must comply with the Manager's password policy, which includes:

- Minimum length and complexity standards (e.g., alphanumeric with special characters)
- Mandatory periodic password changes
- Enforced password history
- Prohibition of password sharing or reuse across critical systems.
- Multi-Factor Authentication (MFA) must be implemented for all privileged accounts and remote access.
- Accounts must be automatically locked out after a defined threshold of failed login attempts (e.g., 5 failed attempts).

c) Periodic Review and Monitoring

- Access rights must be reviewed at least every six (6) months to ensure alignment with current roles and responsibilities
- Departed employees' or contractors' access must be disabled immediately upon termination of employment or engagement.
- System logs (e.g., active directory, financial systems) must be regularly reviewed to detect unusual or unauthorised activities.

Any anomalies or potential breaches of the Guidelines or regulatory requirements shall be escalated by the Responsible Person with remediation actions to the Head of Legal and Compliance of the Manager, the CEO, the RSC and where applicable, to the Board.

d) Privileged Access Management (PAM)

- Privileged accounts (e.g., system administrators, finance system super-users) must be strictly controlled, documented, and subject to enhanced monitoring.
- Activities performed under privileged accounts must be logged and periodically reviewed.
- Shared accounts are prohibited unless technically unavoidable, in which case strict monitoring and approval are required.

e) Regulatory and Oversight Alignment

- Access controls must comply with regulatory expectations, including the Guidelines, applicable regulatory requirements, and the Main Market Listing Requirements of Bursa Malaysia Securities Berhad ("Bursa Securities").
- The IT service provider may, on a risk-based and proportionate basis, be required to provide annual assurance that access control safeguards are aligned with recognised industry standards, commensurate with the criticality of the outsourced systems or services (e.g. ISO/IEC 27001, ISAE 3402 / SOC 1 or SOC 2, or equivalent management assurance).
- Internal audit shall periodically review access control processes for adequacy and effectiveness.

4. DESKTOP, MOBILE COMPUTING DEVICE & STORAGE DEVICE USAGE

The Manager is committed to ensuring that all endpoint devices are securely managed, used responsibly, and aligned with professional and ethical standards. This protects against data loss, operational risks, and reputational harm.

a) Device Governance

- All purchases of endpoint devices must be approved by the respective supervisor/head of department and registered in the IT asset management system.
- Devices must comply with the IT department's hardware standards, be tagged before deployment, and remain under the custody of authorised employees.
- All devices must be returned to the designated IT function or personnel upon resignation, termination, contract expiry, or transfer.
- Lost or stolen devices must be reported immediately to the respective head of department and Responsible Person.
- Any issues or needs for replacements must be reported to IT in a timely manner.

b) Responsible Use and Security

- Users must comply with the Code of Conduct and Business Ethics when using devices.
- Installation of pirated, unlicensed, or unauthorised software is strictly prohibited. Privately owned devices may not connect to the corporate network unless evaluated and approved by IT.
- Users are responsible for the security of the Manager-provided devices regardless of location (office, project site, remote).

c) Data Transmission and Storage

- Secure methods (e.g., encryption, TLS/SSL, SSL VPN) must be used when transmitting sensitive or confidential data.
- Removable storage devices (e.g., USB, external drives) must not contain unencrypted sensitive or confidential data.
- Storage devices no longer in use must be returned to IT for redeployment or safe disposal.

5. BACKUP, RESTORATION AND RESTORATION TESTING

a) Backup Management

- All critical systems must be subject to daily automated backups, with periodic full backups performed at least weekly.
- Backups must be encrypted, securely stored, and segregated from primary systems (e.g., off-site or cloud-based secure locations) to reduce single-point-of-failure risks.
- Retention schedules shall be defined based on regulatory and business requirements, with a minimum retention period of seven (7) years for financial records and key operational data.
- Backup access shall be restricted to authorised IT staff or service providers, with access logs maintained.

b) Restoration Procedures

- Restoration processes must be clearly documented in detailed procedures and tested against defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Only validated backup sets shall be used for restoration, with integrity checks conducted prior to activation.
- Restoration events must be logged, reviewed, and reported to the IT function and Responsible Person for oversight.
- In the event of a recovery (e.g., financial system crash, impaired services arising from technology incident, cyber incident or tenant management data loss), the Responsible Person must promptly notify to the Head of Legal and Compliance and CEO of the Manager, the RSC, and where applicable, to the Board. A notification must be filed to the SC in accordance with the manner prescribed under the Guidelines.

c) Restoration Testing

- Restoration testing shall be conducted at least annually, covering both partial and full system recovery scenarios.
- Testing shall include validation of data completeness, user access rights, system configurations, and application integrity.
- Test results, including any deficiencies and remediation actions, must be documented and presented to the CEO and reported to the RSC and, where applicable, to the Board.
- Critical outsourced service providers (e.g., IT hosting, cloud storage) must provide annual certification of their backup and restoration testing in alignment with the Manager's framework.

d) Escalation and Reporting

- Any failure of backup or restoration testing must be escalated to the Responsible Person with a remediation timeline.
- Significant incidents (including but not limited to technology incidents, cyber incidents or prior to implementing any major technology-related services or major enhancement on its critical systems, that may potentially affect its business operations or may compromise financial

reporting, investor disclosures, or tenant/operational data must be reported to the SC through the Responsible Person in line with applicable regulatory requirements.

6. CYBERSECURITY RISK MONITORING

The Manager shall ensure that its appointed IT service providers, as well as internal IT governance standards and practices, establish adequate cybersecurity controls, which include:

- Cyber risk identification and monitoring.
- Incident detection, response, and recovery.
- Protection of business-critical systems and data.
- Ongoing assessment of technology vulnerabilities.

The Manager shall obtain assurance that such measures are, at a minimum, in line with the Guidelines.

Where necessary, the Manager may implement additional cybersecurity measures commensurate with the business model, risk appetite, reliance on technology, and compliance with applicable laws and regulations.

7. CYBERSECURITY ESCALATION

The Manager shall establish and maintain escalation and reporting procedures for cybersecurity incidents in line with the Board's risk appetite, regulatory expectations and best practices. This includes, but is not limited to, requirements for escalation to the Head of Legal and Compliance, the RSC and, where applicable, the Board and a notification to the SC and Bursa Securities for the following:

- Notification for Technology-Related Implementation.
- Notification of Cybersecurity Incidents or Near Miss Events.

8. IT OUTSOURCING

All outsourcing of critical IT functions must be subject to due diligence, contractual safeguards, and Board-approved oversight, which is at a minimum in accordance with the Guidelines. This includes:

- Service providers must demonstrate compliance with the Guidelines, for applicable areas.
- Contracts must include key provisions such as cybersecurity standards, business continuity and disaster recovery capabilities, data confidentiality and ownership, among others.
- The Responsible Person will monitor outsourced IT vendor performance, with material breaches escalated to the CEO and the Head of Legal and Compliance of the Manager.

This section shall be read together with the Outsourcing Management Policy.

9. TECHNOLOGY PROJECT MANAGEMENT

a) The Manager shall establish clear internal guidelines for technology-related projects, covering planning, approval, implementation, and post-completion evaluation.
b) Project risk assessments must be conducted at all stages of the project lifecycle to identify risks relating to delivery, cost, quality, and security.
c) Post Implementation Reviews (PIRs) shall be performed for all critical projects. Lessons learned must be documented and incorporated into future projects.
d) Adequate personnel, including project coordinators and advisors, must be assigned to oversee project costs, schedules, deliverables, and risks.

10. SYSTEM ACQUISITION AND DEVELOPMENT

All new systems or significant upgrades must follow a defined System Development Life Cycle ("SDLC"), encompassing planning, requirement analysis, design, implementation, testing, and acceptance. Requirements include:

- Vendor selection and evaluation.
- Secure software development practices (internal or external).
- Incorporation of security controls (access, data integrity, confidentiality, logging, and exception handling).

Where feasible, source code escrow agreements should be executed to safeguard continuity. If not feasible, appropriate alternatives must be identified.

Security requirements must be embedded throughout the SDLC to minimise vulnerabilities.

11. SYSTEM TESTING AND ACCEPTANCE

a) Rigorous testing must be conducted before deployment, covering business logic, functionality, controls, and performance under stress conditions.
b) Automated testing tools should be used, where feasible, to strengthen coverage.
c) All vulnerabilities, deficiencies, or system bugs identified during testing must be documented, tracked, and remediated.
d) Cybersecurity assessments must be performed before deployment, commensurate with the system's risk profile.
e) Final acceptance testing (technical assurance) and user acceptance testing (functional assurance) must be completed and results reported to senior management before production rollout.
f) For acquired systems, only the only the final, vendor-approved version shall be implemented.

12. REVIEW AND AUDIT OF IT, TECHNOLOGY AND CYBERSECURITY

The Manager will ensure that all IT, technology, and cybersecurity measures are subject to periodic review and audit to maintain resilience, compliance, and alignment with industry best practices and standards.

a) Annual Independent Review

- The review must be conducted on the Manager's IT systems and technology infrastructure including access controls, device usage, information security practices, and cyber risk management.
- The review must benchmark against industry best practices and, at a minimum, comply with the Guidelines.
- The review must assess alignment with the Manager's business model, risk appetite, and level of technology dependency.

b) IT, Technology and Cybersecurity Audit

The Manager shall appoint a qualified and independent auditor (internal or external) to conduct a technology audit at least once every two (2) years. The audit scope shall, at a minimum, cover:

- Compliance with the Guidelines, applicable laws, regulations and industry practices and standards.
- Confidentiality, integrity, and availability of data and information systems.
- Efficiency and effectiveness of IT service provider operations.
- Cyber incident detection, escalation, and remediation practices.

Audit findings shall be presented to the relevant governance bodies for appropriate oversight and deliberation, namely the RSC in respect of risk management matters, the Audit Committee of the Manager in relation to internal control systems, and the Board for overall governance and accountability.

c) Additional Testing and Assurance

- Penetration testing and vulnerability assessments must be conducted at least annually or at such other interval based on management's and the Board's risk assessment.
- Restoration testing for critical systems must be incorporated into reviews to validate RTOs and RPOs.
- Annual assurance from outsourced IT service providers must be obtained, confirming compliance with the Policy and the Guidelines.
- Results of all reviews and tests must be documented, with significant risks escalated to the RSC, the Board and, where there are material breaches, reported to the SC and Bursa Securities pursuant to the Guidelines and other relevant applicable statutory requirements.

13. IT DISASTER RECOVERY PROCEDURES

The Manager, together with its IT service providers, shall establish and maintain an IT Disaster Recovery Procedure (DRP) to ensure operational resilience in the event of major technology disruptions. The DRP shall be reviewed at least annually and benchmarked against the Guidelines.

Key elements of the IT DRP include:

- Risk Assessment: Identification of critical systems and data, potential failure scenarios, and single points of failure.
- Business Impact Analysis (BIA): Assessment of maximum tolerable downtime (MTD), RTOs, and RPOs.
- Crisis Management Structure: Clear roles, responsibilities, and escalation protocols for management, IT, and service providers.
- Data Backup and Recovery: Defined procedures for data replication, secure off-site/cloud storage, and restoration testing.
- Alternate Site and Infrastructure: Arrangements for backup servers, facilities, or cloud environments to support recovery.
- Communication Procedures: Internal and external communication plans, including notification to regulators, unitholders, and stakeholders, where material.
- Testing and Drills: Periodic simulation exercises (at least periodically) to validate readiness of IT staff, service providers, and systems.

Documentation and Continuous Improvement: DRP must be fully documented, tested, updated for new risks, and lessons learned incorporated.

14. TRAINING AND AWARENESS

The Manager recognises that employees, management, and directors play a critical role in technology management, particularly, cybersecurity resilience. Accordingly:

- Cybersecurity and technology risk awareness programmes shall be conducted at least annually for directors, employees and any other relevant users.
- Training shall be tailored to responsibilities/job functions (e.g. phishing awareness for staff, governance oversight for directors).

- New or emerging trends in technology risk and cyber threats shall be reported to the Board and disseminated to employees in a timely manner.
- The Responsible Person and IT function shall collaborate to ensure continuous updates on regulatory changes, cyber incidents, and lessons learned.

15. POLICY MAINTENANCE

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 technology risks, regulatory requirements, industry best practices, and any material changes in applicable laws, regulations, or the Manager's business operations.