# IT GENERAL CONTROLS POLICY

**Meridian Financial Services Inc.**

Document Ref: MFSI-IT-GC-POL-001 | Version: 3.1 | Classification: CONFIDENTIAL

## Version Control

| Version | Date | Author | Description | Status |
|---|---|---|---|---|
| 1.0 | 14 Mar 2021 | D. Asante (Head of IT Ops) | Initial policy drafted for Series B compliance programme | Approved |
| 2.0 | 09 Jan 2023 | D. Asante (Head of IT Ops) | Expanded change management section. Added emergency change retrospective requirement. | Approved |
| 3.0 | 02 Oct 2023 | F. Mensah (IT Risk Manager) | Added privileged access section. Updated backup retention to align with SOX guidance. | Approved |
| 3.1 | 18 Mar 2024 | F. Mensah (IT Risk Manager) | Quarterly privileged access review requirement added. Minor formatting updates. | Approved |

## Approval and Sign-Off

| Role | Name | Signature | Date |
|---|---|---|---|
| Chief Technology Officer | A. Boateng | _____ | 18 Mar 2024 |
| Head of IT Operations | D. Asante | _____ | 18 Mar 2024 |
| Chief Financial Officer | O. Mensah | _____ | |
| Internal Audit — IT Lead | | _____ | |

*GAP: The CFO sign-off column is blank — finance approval of IT controls policy has not been obtained. The Internal Audit sign-off is also missing, meaning no independent review of this policy has been completed prior to approval.*

## 1. Purpose

This policy establishes minimum requirements for IT General Controls (ITGCs) across Meridian Financial Services Inc. ("Meridian" or "the Organisation") in support of the Organisation's preparation for Sarbanes-Oxley (SOX) Section 404 compliance ahead of its planned initial public offering (IPO). ITGCs provide the foundation upon which application controls and financial reporting processes depend. Without effective ITGCs, the reliability of automated application controls and the integrity of financial data cannot be assured.

## 2. Scope

This policy applies to all systems, personnel, and third-party service providers that support Meridian's financial reporting environment, including:

- Core transaction processing platform (TXN-Core v4.2)
- Enterprise Resource Planning system (Oracle Fusion)
- Identity and Access Management system (Okta)
- Source code management and deployment pipeline (GitHub / Jenkins)
- Backup infrastructure (Veeam + offsite tape rotation)
- Network infrastructure (Cisco / Palo Alto)
- All cloud environments hosting in-scope systems (AWS us-east-1)

> **AUDIT NOTE — DELIBERATE GAP**
> *SCOPE GAP: This policy does not specify a formal in-scope / out-of-scope determination methodology. Systems supporting financial reporting that were deployed after the last scope review (March 2023) — including the new Payment Reconciliation Module (PRM, deployed November 2023) — may not have been formally assessed for ITGC scope inclusion.*

## 3. Definitions

**Privileged Account:** An account with elevated system rights including administrator, system, service, database administrator (DBA), or root access.

**Segregation of Duties (SoD):** The separation of incompatible responsibilities among different individuals to prevent or detect errors and irregularities.

**Change Advisory Board (CAB):** The body responsible for reviewing and approving changes to production systems.

**Emergency Change:** An unplanned change required to restore service or address an immediate security risk that cannot wait for the next scheduled CAB review.

**Recovery Time Objective (RTO):** The maximum acceptable duration within which a system must be restored following a failure.

**Recovery Point Objective (RPO):** The maximum acceptable period of data loss measured in time.

**Joiner-Mover-Leaver (JML):** The process covering onboarding (Joiner), role changes (Mover), and offboarding (Leaver) of staff with system access.

## 4. User Access Management

### 4.1 Provisioning

Access to all in-scope systems must be formally requested using the IT Service Desk ticketing system (ServiceNow). All access requests require written approval from the requesting user's direct line manager. Requests for privileged

access require additional written approval from the Head of IT Operations. New user accounts must be created within **5 business days** of the employee's confirmed start date.

> **AUDIT NOTE — DELIBERATE GAP**
> *PROVISIONING GAP: The 5-business-day SLA applies to account creation, not access activation. No SLA exists for provisioning access to specific applications once an account is created. Users have been found active in financial systems before their formal onboarding documentation was completed.*

### 4.2 User Termination

Upon notification of an employee termination, IT Operations must disable all in-scope system access **within 48 hours** of the termination effective date. Human Resources (HR) is responsible for notifying IT Operations of all terminations via the IT Service Desk. Notification must be submitted no later than the close of business on the termination date.

> **AUDIT NOTE — DELIBERATE GAP**
> *TERMINATION GAPS: (1) This policy does not distinguish between voluntary and involuntary terminations. Industry best practice and many regulatory frameworks require same-day (immediate) access revocation for involuntary exits due to the elevated risk of retaliatory or malicious access. (2) No SLA exists for revoking access for contractors, consultants, or third-party personnel — only permanent employees are addressed. (3) HR notification is via email only, with no read-receipt or escalation mechanism. If the IT Service Desk does not action the email, there is no compensating alerting control.*

### 4.3 Access Reviews

IT management shall conduct a formal review of all user access rights on a **semi-annual basis** (every six months). Reviews must be initiated within the first 5 business days of the review period and completed within 30 calendar days. Access review results, including certifier decisions and any remediation actions, must be documented and retained for a minimum of **two years**. Privileged access accounts must be subject to a separate **quarterly** access review.

> **AUDIT NOTE — DELIBERATE GAP**
> *ACCESS REVIEW GAPS: (1) This policy does not specify who is responsible for certifying access — whether the certifier is the user's line manager, the system owner, or IT. Without a named certifier, accountability for inaccurate certifications cannot be assigned. (2) No escalation procedure is defined for certifiers who do not respond within the review window. (3) The policy does not require that access removed during a review is actioned within a specific timeframe after the review is completed — a gap between certification and remediation may exist. (4) There is no requirement to perform an access review following a significant organisational change (e.g. restructuring, acquisition).*

### 4.4 Segregation of Duties (SoD)

No single user shall hold the capability to both initiate and approve financial transactions above **$10,000**. IT shall maintain a Segregation of Duties (SoD) conflict matrix that identifies incompatible role combinations across all in-scope financial systems. The SoD matrix must be reviewed and updated **annually**, or upon any significant change to system roles or business processes. Where SoD conflicts are identified, they must be remediated or formally accepted with compensating controls.

> **AUDIT NOTE — DELIBERATE GAP**
> *SOD GAPS: (1) The SoD matrix is referenced but is not attached to or formally governed by this policy. No policy owner is responsible for maintaining the SoD matrix. (2) No compensating controls are defined for situations where SoD conflicts cannot be eliminated due to staffing constraints (e.g. small teams). Acceptance of SoD conflicts is not documented. (3) No automated SoD monitoring or alerting is required — conflicts may exist between reviews without detection. (4) The $10,000 threshold for transaction initiation/approval SoD has not been reviewed since policy v1.0 and does not reflect Meridian's current transaction volumes.*

## 5. Change Management

### 5.1 Change Classification

All changes to production systems must be classified as one of the following:

- **Standard Change** — Pre-approved, low-risk, follows a fully documented and repeatable procedure. No CAB approval required.
- **Normal Change** — Planned change that requires Change Advisory Board (CAB) review and approval prior to implementation.
- **Emergency Change** — Urgent change required to restore service or mitigate a critical security risk. Post-implementation retrospective approval required.

### 5.2 Change Approval

Normal changes require approval from at least **one member of the CAB** before implementation. The CAB meets on a **bi-weekly basis** to review and approve pending change requests. Emergency changes must be approved verbally by the Head of IT Operations or CTO prior to implementation, with written retrospective approval documented in the change management system within **5 business days** of implementation.

> **AUDIT NOTE — DELIBERATE GAP**
> *CHANGE APPROVAL GAPS: (1) This policy does not prohibit developers or engineers from deploying their own changes to the production environment. A developer may both implement and approve their own change — a fundamental SoD failure in the change management process. (2) Emergency change retrospective reviews have no defined quality criteria — there is no requirement for the retrospective to assess whether the change was truly an emergency or whether normal process could have been followed. (3) CAB membership, quorum requirements, and voting thresholds are not defined in this policy.*

### 5.3 Testing Requirements

All normal changes must be tested in a designated non-production environment before production deployment. Test results, including test scenarios executed, expected results, and actual outcomes, must be documented and retained as evidence. The system owner or a designated tester must formally approve test results before production deployment proceeds.

> **AUDIT NOTE — DELIBERATE GAP**
> *TESTING GAP: Emergency changes may bypass non-production testing with Head of IT Operations approval, provided a rollback plan is documented. However, no requirement exists to complete post-implementation testing in production following an emergency change to confirm the change achieved its intended effect without introducing unintended consequences.*

## 6. Backup and Recovery

### 6.1 Backup Schedule

All in-scope critical systems must be backed up on a daily basis. The backup schedule is as follows:

- Full system backup: Every Sunday, commencing no later than 22:00 local time
- Incremental backup: Monday through Saturday, commencing no later than 23:00 local time
- Backup logs must be reviewed by IT Operations on a weekly basis
- Failed backups must be remediated within 24 hours of identification

> **AUDIT NOTE — DELIBERATE GAP**
> *BACKUP GAPS: (1) This policy does not specify who is responsible for reviewing backup logs or what constitutes a backup failure requiring escalation. (2) No SLA exists for remediating failed backups — the 24-hour remediation window in the schedule above does not appear in the policy text and is therefore not enforceable. (3) No requirement exists for backup monitoring alerts — a failed backup may not be detected until the weekly log review, potentially 7 days later.*

### 6.2 Restore Testing

Restore tests must be conducted **annually** to verify the integrity and recoverability of backup data. Test results must be documented, including the system tested, data restored, test date, and tester identity. Restore test documentation must be retained for a minimum of two years.

> **AUDIT NOTE — DELIBERATE GAP**
> *RESTORE TESTING GAPS: (1) Annual restore testing frequency is widely considered insufficient for a SOX-regulated financial services environment. Industry best practice and many audit frameworks recommend quarterly restore testing for critical financial systems. (2) This policy does not require testing of restoration for specific financial data sets or transaction records — a system may be restored from backup without verifying that financial data is complete and accurate. (3) No independent witness or reviewer is required for restore tests — the same person who performs the test may also document and approve the result.*

### 6.3 Retention and Offsite Storage

Backup media must be retained for a minimum of **90 days**. Offsite or cloud storage is required for disaster recovery purposes. Backup media must be encrypted during storage and transport.

## 7. Privileged Access Management

Privileged accounts — including system administrators, database administrators (DBAs), network administrators, and cloud IAM administrators — are subject to the following enhanced controls:

- Multi-factor authentication (MFA) is **recommended** for all privileged accounts
- Privileged account activity must be logged and log data retained for a minimum of 12 months
- Shared or generic privileged accounts are **discouraged**; where they exist, their use must be justified in writing
- Privileged accounts must be reviewed on a **quarterly** basis

**AUDIT NOTE — DELIBERATE GAP**

*PRIVILEGED ACCESS GAPS: (1) MFA is stated as "recommended" rather than "required" for privileged accounts. This is a critical gap for a SOX environment — privileged access without mandatory MFA represents a significant authentication control weakness. Most SOX auditors will treat this as a control deficiency. (2) Shared/generic privileged accounts are "discouraged" but not prohibited. Where they exist, individual accountability for privileged actions cannot be established. (3) Privileged access logs must exist, but no monitoring, alerting, or review requirement is specified — logs may exist but never be reviewed. (4) No requirement for Privileged Access Workstations (PAWs), just-in-time (JIT) access, or privileged access management (PAM) tooling.*

## 8. Incident Management

Security incidents must be reported to the IT Service Desk within **24 hours** of detection. Major incidents (Priority 1) must be escalated to the CISO and Head of IT Operations within **4 hours** of identification. A post-incident review (PIR) must be completed for all Priority 1 incidents within **10 business days** of resolution.

## 9. Policy Exceptions

Exceptions to this policy must be approved in writing by the Head of IT Operations and documented in the Policy Exception Register. Exceptions are valid for a maximum of **6 months** and must be reviewed and re-approved before expiry. All exceptions must include a documented risk assessment and details of any compensating controls in place.

**AUDIT NOTE — DELIBERATE GAP**

*EXCEPTION PROCESS GAP: The Policy Exception Register is referenced but no owner, storage location, or review cadence is defined. There is no requirement for exceptions to be reported to senior management or the board, and no mechanism to track exceptions approaching their expiry date.*

## 10. Compliance and Enforcement

Non-compliance with this policy may result in disciplinary action up to and including termination of employment. Repeated or wilful non-compliance involving in-scope financial systems may be reported to the Audit Committee. This policy is reviewed annually. The next scheduled review is **March 2025**.