The Future Is Better Together

OS UPDATE PLAN
Version 1.0

TECHNICAL DIRECTORATE

Document Details

Table 1 Document Properties

Document Property	
Prepared by	Portia M Bobo
Project Title	OS Update Plan Q3
Reference	TEL-ISHN-PLAN-001
Version number	1.0
Document Classification	**Internal**
First Creation Date	17 July 2025
Owner	System Administrator
Next Review Date	October 2025

Version Management

Table 2 Version History

Version	Date	Author	Nature of Amendment
1.0	17/July 2025	Portia M Bobo	• OS update plan Draft

Table of Contents

Definition of Terms

In this process:

"ISO/IEC 27001:2022": An international standard for information security management systems (ISMS).

"CR": Change Request – a formal proposal for an alteration to the IT environment.

"VM": Virtual Machine – emulated computing system hosted on a physical server.

"Patch": Software update intended to fix vulnerabilities or improve performance.

"Rollback": Process of reverting a system to its previous stable state.

Introduction

This document defines the structured plan for deploying security patches and system updates across TelOne's internal Windows Server infrastructure. The objective is to maintain system integrity, availability, and confidentiality in compliance with ISO/IEC 27001:2022 controls.

Scope

Applies to: All internal production and test Windows Servers used within TelOne's IT ecosystem.

Excludes: Third-party-managed systems unless under specific SLA clauses.

a) Mitigate vulnerabilities by applying critical and security updates.
b) Maintain system availability and compliance with ISO/IEC 27001 Annex A control A.12.6.1 (Management of technical vulnerabilities).
c) Ensure system owners participate in post-update validation.

Roles and Responsibilities

System Owners: Validate system functionality after updates.

IT Operations Team: Schedule, implement, monitor, and report on updates.

Information System Team: Approve updates and verify compliance with patch management policies.

Update Strategy

Updates will be performed in 3 Phases to minimize downtime and isolate issues. Testing will begin with non-critical systems in each phase to validate stability before updating business-critical servers.

Phase 1 – 04/08/2025

a) Host 172.27.33.2 which hosts the following sytems
   i.   Kiosk_System
   ii. OTP svr 1
   iii. Payment_gateway_iveri
   iv. Solutions Test Environment
   v.   Tomi Migrated VM
b) Host 172.27.33.3 which hosts the following systems
   i.   Backend Smart Wifi
   ii. Notification Engine 1

Phase 2 – 13/08/2025

a) Host 172.27.33.4 which hosts the following sytems
   i.   API Banks
   ii. Digital Shop 2
   iii. E -Recruitment
   iv. E-Recruitment Administrator
   v.   Mobile App (USSD)
b) Host 172.27.33.8 which hosts the following sytems
   i.   App Dev-Staging
   ii.   Canteen Server
   iii. ClientPortal
   iv.   Cpanel DR
   v.   Customer Onboarding
   vi.   Fiscal03
   vii. Fiscal04
   viii. OTR SVR2
   ix.   PublisherPortal

      x.   Solutions systems

      xi.   Tomi Test

c) Host 172.27.33.6 which hosts the following sytems
   - i.   Digital shop client
   - ii.   IS AUDIT
   - iii. Tel-svc

Phase 3 – 10/10/2025

a) Host 172.27.32.54 which hosts the following sytems
   - i.   Belina
   - ii.   Belina02
   - iii.   Customer On Boarding
   - iv.   Data Warehouse
   - v.   Digital Shop Client 2024
   - vi.   Digital Shop Solution
   - vii.   Domain Controller 4
   - viii. EVD APP
   - ix.   EVD DB
   - x.   Exchange Web Server
   - xi.   Fiscal
   - xii.   Fiscal FDMS
   - xiii. Fiscal02_replica
   - xiv. Op Manager01
   - xv.   Oracle Test
   - xvi. Payment Gataeways
   - xvii. Payment Integrations Development
   - xviii. PERFORMANCE-MGT
   - xix. QliksenseClone
   - xx.   Solution Test
   - xxi. Starlink Server
   - xxii. Spamtitan
   - xxiii. Spring API
   - xxiv. Telpay Restore
   - xxv. Tenable Nessus VM
   - xxvi. TOMI
   - xxvii. TOMI TEST
   - xxviii. Unbundling DB
   - xxix. USSD

xxx.   VMS.telOne

xxxi.   Website

xxxii.   Workflow VM

xxxiii. Zitco webx

Backup Plan

All affected Virtual Machines will be fully backed up. Backup logs will be reviewed and verified by the IT Operations team.

Communication Plan

a) Change Requests: Official change requests (CRs) will be raised, approved, and circulated.

b) Internal Notifications: System owners will receive notice at least 3 business days in advance. Client-Facing Platforms: The Call Centre will be informed to prepare for any potential client impact.

Post-Update Monitoring

a) All systems will undergo 24-hour monitoring post-update.

b) Metrics tracked: CPU, RAM, Disk I/O, Application Errors.

c) Anomalies or system issues will be escalated immediately with logs attached.

Reporting and Documentation

A patch report will be generated after each phase, documenting:

a) Servers updated

b) Issues encountered

c) Rollbacks (if any)

Reports will be submitted to the Information System Manager.

Rollback Plan

Each system has a documented rollback procedure using pre-update VM snapshots.

Rollbacks will be executed only if:

a) Core functionality is disrupted
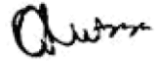
b) Security controls are compromised

Incidents requiring rollback will be logged as security events per ISO/IEC 27001:2022 Annex A.16.

Next Planned Update Cycle

Mid October 2025

Document Approval

By signing below, the individuals acknowledge that they have created, reviewed, or approved this document.

	Name: Position	Date	Signature
Created By			
Reviewed By			
Approved By	Tichaona Chisvuure: Information System Infrastructure Manager	21/07/2025	
Approved By	Annamercy Jaratina: Customer Service Applications Manager	23/07/2025	Ashiri
Approved By	Easylin Muganda: Information Systems Security Manager	23/07/2025	
Approved By	Gracious Chinyama: Solution Development Manager	24/07/2025	
Approved By	Head Information Systems	06/08/2025	
Approved By	Head Innovation	22/08/2025	
Approved By	Head Client Services	06/08/25	