Executive Summary
IT General Policy

DUOPHARMA

INTRODUCTION

At Duopharma, information technology (IT) resources including hardware, software, networks, and data are vital assets that support our mission of providing **Smarter Solutions for a Healthier Life**.

This policy establishes a mandatory framework to ensure these resources are used effectively, securely, and in alignment with regulatory standards.

Our goal is to protect the **confidentiality, integrity, and availability** of information against evolving cybersecurity threats.

ACCOUNTABILITY MATRIX

DUOPHARMA

IT Department

(The Architects)

- Provision & secure equipment
- Enforce MFA and firewalls
- Maintain asset tracking
- Investigate breaches

Heads of Department

(The Enforcers)

- Ensure team compliance
- Act as first-line contact for IT concerns
- Validate user access needs

Employees & Users

(The Frontline)

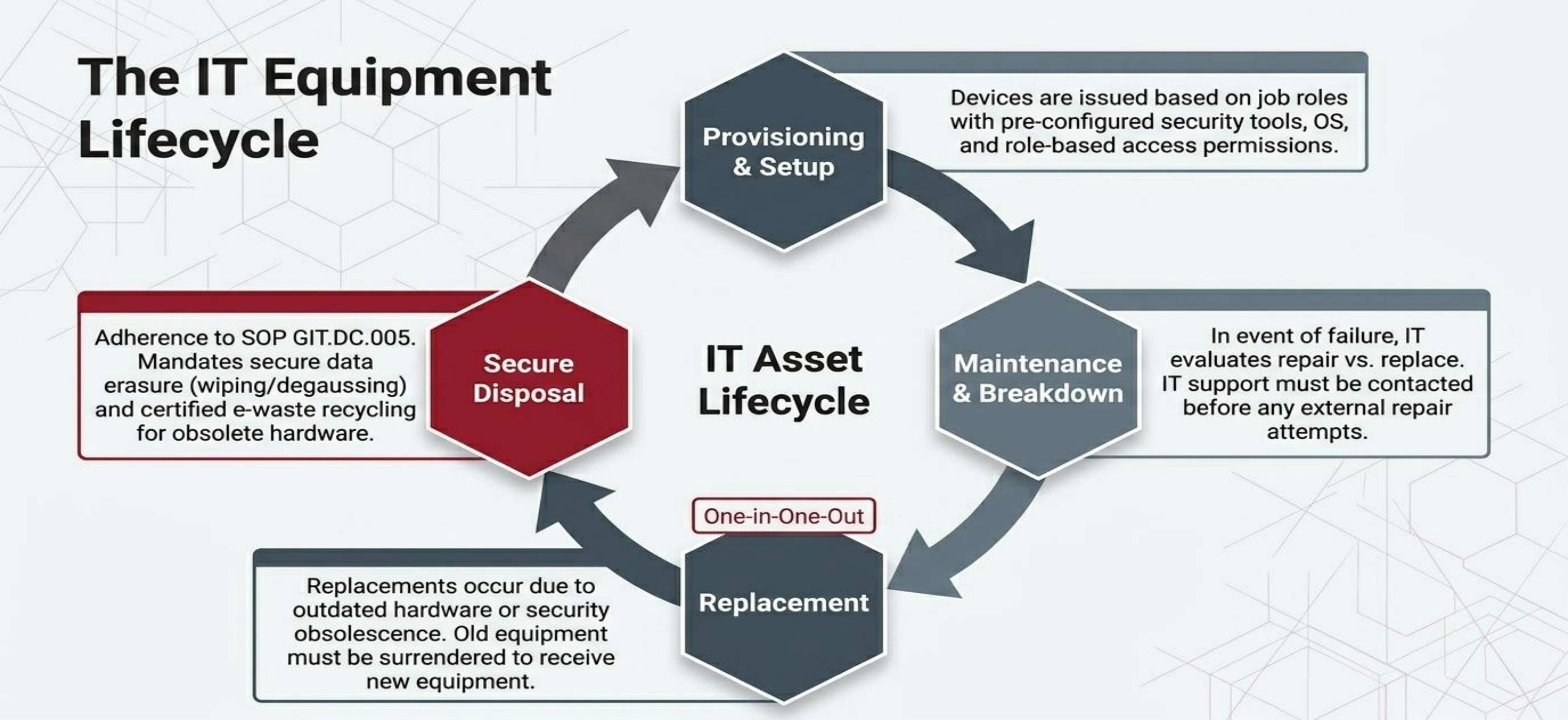
- Protect credentials/devices
- Use equipment for organizational purposes
- Immediately report losses or anomalies

Third-Party Vendors

(The Partners)

- Sign data protection agreements
- Adhere strictly to access limitations
- Report any compliance breaches

IT ASSET EQUIPMENT LIFECYCLE



RULES OF ENGAGEMENT : IT USAGE

DUOPHARMA

Acceptable Use

Exclusive use for work-related tasks and organizational purposes.

Securing devices with strong passwords and locking screens when unattended.

Connecting only to trusted networks (avoiding public Wi-Fi for confidential work).

Prohibited Use

Bypassing internet filtering or disabling security controls.

Installing unauthorized software or downloading illegal/pirated content.

Excessive personal use that degrades network performance (e.g., media streaming).

Using public IT infrastructure for any illegal, defamatory, or harassing activity.

THE BYOD FRAMEWORK

DUOPHARMA

The BYOD Checkpoint Model

The Device

Personal smartphones, tablets, or laptops used for business.

The Security Filter

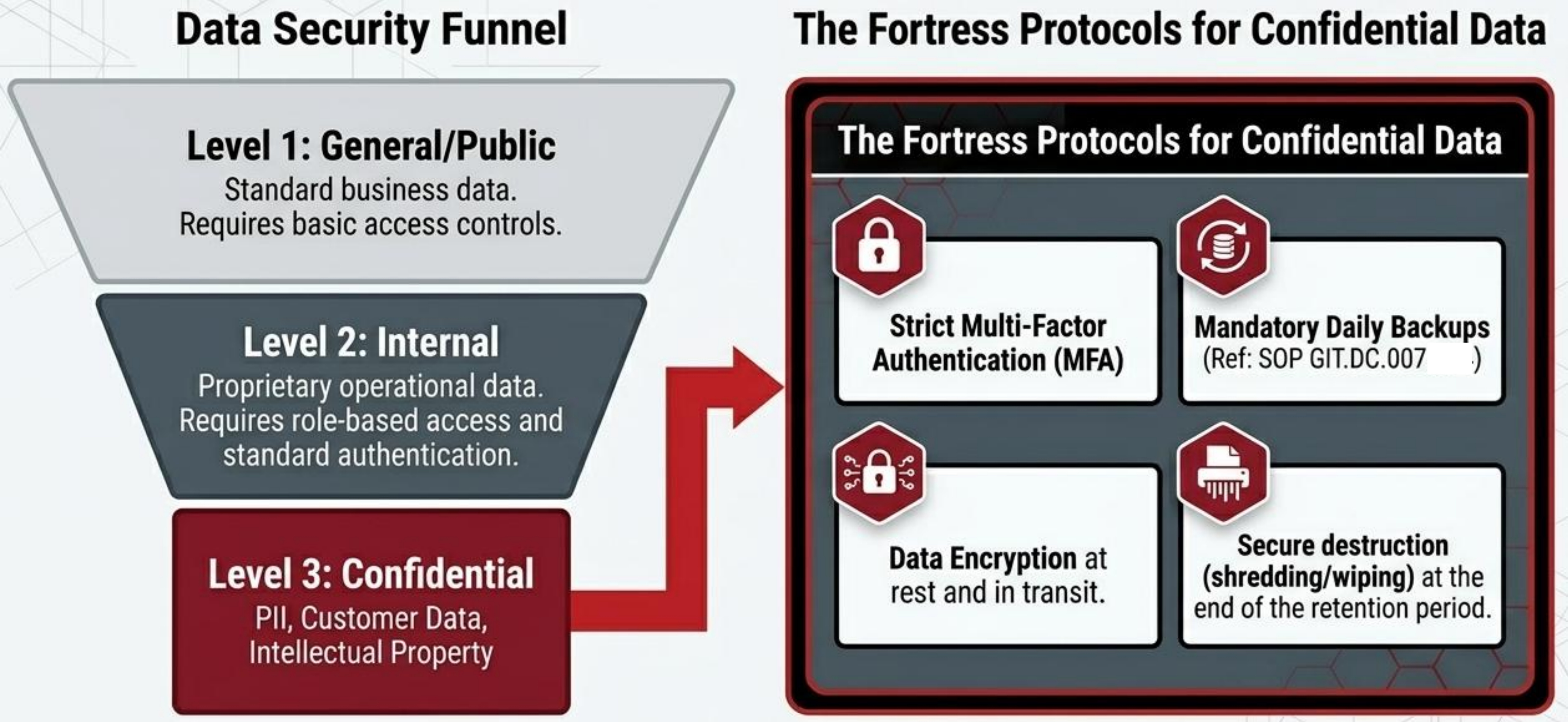
- Must use strong passwords or biometric authentication.
- Data encryption required for sensitive information.
- Explicit IT approval required for internal system access.

Duopharma Secure Network

The Mandate: IT Intervention Rights

By opting into BYOD, users grant IT the right to wipe company data remotely in three scenarios: Loss/Theft, Termination of Employment, or Severe Policy Violation.

DATA PROTECTION & CLASSIFICATION



NETWORK & ACCESS SECURITY

DUOPHARMA

Remote Access Security

All remote connections (VPN) require MFA. Automated session timeouts enforce disconnection after predefined inactivity periods.

Logical Access Control

Governed by the Principle of Least Privilege.

Access rights are dynamically reviewed and immediately revoked upon role change.

Physical & Network Architecture

Physical access to IT facilities (server rooms) is strictly controlled.

Networks are segmented with firewalls to prevent unauthorized lateral movement.

CRITICAL EVENT PROTOCOLS

DUOPHARMA

Damage, Loss, or Theft

Step 1: Immediately notify IT Helpdesk and Security.

Step 2: If stolen, file a local police report and obtain a case number.

Step 3: Do not attempt unauthorized repairs (voids warranties).

Resignation or Termination

Step 1: Ensure all company data is backed up to secure departmental drives.

Step 2: Return all hardware & accessories on or before the last working day.

Step 3: CRITICAL: Do NOT factory reset or wipe the device yourself; devices must be returned in original state for IT processing.

THANK YOU

DUOPHARMA

Smarter Solutions. Healthier Life.