



# Google Workspace Multi-Factor Authentication (MFA) Policy

**Document ID:** DTT-IT-POL-005

**Issuing Department:** Digital Transformation

**Information Classification:** For Internal Use Only

**Version:** 1.0

**Issued By:** John Lester Rosima - IT Assistant Manager Cybersec/IT Projects

**Effective Date:** June 1, 2026

## 1.0 Purpose & Scope

This policy establishes multi-factor authentication (MFA) as a mandatory security layer for all sign-ins to the company's Google Workspace environment. Requiring MFA significantly reduces the risk of unauthorized access even if passwords are compromised, providing an additional layer of defense against credential theft and phishing attacks.

This policy applies strictly to all employees who are provisioned with a corporate email account, network credentials, or access to Oak Drive Ventures, Inc. (ODVI) Google Workspace services.



## 2.0 Roles & Responsibilities

Information security is a shared corporate responsibility. The roles defined below must work together to maintain account integrity:

| Role                                                           | Responsibility                                                                                                                                                                                           |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DTT IT                                                         | Configure MFA settings in the Google Admin Console, monitor system-wide compliance, assist employees with enrollment, and evaluate valid exemption requests.                                             |
| Backup Person<br><br>(Dolden<br>Modesto &<br>Charlene<br>Mago) | Act as the designated backup to assist with MFA configurations, troubleshooting, and user support when the primary personnel are unavailable, out of the office, or unable to provide immediate support. |
| Employees                                                      | Complete MFA enrollment using approved methods, safeguard backup authentication choices, and report any suspicious authentication prompts immediately.                                                   |
| Management                                                     | Ensure all direct team members complete enrollment and comply fully with the authentication standards outlined in this policy.                                                                           |



### 3.0 MFA Configuration & Rules

To maintain access to corporate communications and files, employees must configure their authentication profiles according to the following specifications:

- **Primary Authentication:** The Google Authenticator mobile application utilizing time-based one-time passwords (TOTP).
- **Backup Authentication:** SMS text verification or phone call verification protocols.
- **Enrollment Requirement:** Employees are prompted to configure MFA upon their first sign-in and must complete setup to access Workspace services. Access to email and drive tools will remain restricted until configuration is finalized.
- **Authorized Exemptions:** Standard employee accounts are not exempt from this policy. Technical exceptions are strictly limited to:
  - Individual accounts with documented, specialized justification explicitly approved by DTT Administrations.

### 4.0 Monitoring & Support

- **Access Oversight:** The Digital Transformation Department (DTT) utilizes the central Google Admin Console to audit configuration logs, trace missing enrollments, and check configuration integrity.
- **Technical Assistance:** The DTT team will provide comprehensive configuration guides for the Google Authenticator application and offer troubleshooting assistance for employees experiencing device synchronization issues.



## 5. Penalties & Violations

Failure to comply with this policy will result in the following disciplinary actions:

- **First Instance:** A verbal reminder or coaching session to help update your settings.
- **Repeated Instances:** A formal written warning and a quick security briefing.
- **Continued Issues:** Disciplinary action as outlined in the Employee Handbook.

Prepared by:

**John Lester Rosima**  
Assistant Manager – Cybersecurity & IT  
Projects.

Reviewed and approved by:

**Michael Singson**  
Chief of Staff