Voice Cloning

&

Impersonation Protection Policy

Internal
V1.0 Updated 23/12/25

1. Purpose and Background

Advancements in artificial intelligence now enable near-perfect replication of any individual’s voice using only a few seconds of publicly available audio. Criminal organisations and state-sponsored actors are actively using AI-generated voice clones in business email compromise (BEC), CEO fraud, vendor impersonation, and emergency data-exfiltration attacks. This policy establishes mandatory, non-discretionary controls to eliminate successful voice-based social-engineering attacks against the Company.

2. Scope

This policy applies to:

- All employees
- All devices and communication channels capable of receiving telephone calls or voice messages on behalf of the Company

3. Core Principle

Never trust a phone call or voice message alone - even if the voice sounds 100 % real.

4. Prohibited Actions

- Executing any financial transaction or invoice, based solely on a phone call
- Sharing passwords, 2FA codes, or granting access in response to a call
- Bypassing normal processes because the caller demands urgency or secrecy

5. **Immediate Red-Flag Scenarios (Assume voice clone until proven otherwise)**

- Urgent money transfer or payment change requests
- Requests to buy gift cards, crypto or send funds
- Asking for passwords, 2 Factor Authentication codes or system access
- “*Off-the-record*” or “*don’t tell anyone*” instruction
- Caller claims to be the boss but you know they are in a meeting, on leave, or in a different time zone
- Any call that creates pressure, fear of consequences, or unusual urgency

6. Mandatory Verification Process

Step 1 – Stay calm. Do NOT act immediately. Politely say, *“Let me verify this request through our secure channel. I will call you back on a known number.”*

Step 2 – Hang up immediately.

Step 3 – Verify using a different communication method

- Call back using a number you already have saved (previous signed email, mobile phone contacts etc). NEVER use the incoming caller ID
- Send an instant message on Email / WhatsApp asking, “Did you just call me?”
- For calls received taking Chairman / CXO / Leadership Teams name, inform your reporting manager immediately

Step 4 – Ask the pre-agreed secret security question / safe word (see Section 7)

Step 5 – Proceed after 100 % positive confirmation

7. Security Questions / Safe Word

Every employee and manager MUST establish at least one secret question/answer known only to immediate team members.

Examples (must be set in advance and kept private):

Question (asked by the employee)	**Answer (pre-agreed)**
What is our company “safe word” for 2026?	Anchor
What is the name of the restaurant opposite our office?	Ego
What is the shared password we use for urgent verifications?	Quick!Safe@23

Note:

- *Never use public information (birthdays, pet names, etc.)*
- *Change every 6 - 12 months and immediately after an employee exit*
- *Store only in the company password manager*
- *Executives and Finance team must have unique questions with each direct report*

8. Handling a voice-clone attack

- Do not share any information
- Immediately report to techescalations@tlcgroup.com and your direct manager
- Record the call if possible and legally permissible
- Forward caller ID, exact time, and duration to IT Security

9. Personal Liability

Any employee who bypasses the mandatory verification procedure and causes loss, will be held solely responsible for:

- Full financial repayment of the loss
- Reputational damage and regulatory penalties
- Immediate termination for gross negligence
- Possible referral to law enforcement

The Company will not indemnify or reimburse employees for losses caused by policy violation.

10. HR Responsibility

- Mandatory training at onboarding and annually
- Quarterly 5-minute refresher
- Policy uploaded on TLC website and emailed to all employees
- Signed acknowledgment required from every individual

Employee Acknowledgment

I have read and fully understand the Voice Cloning and Impersonation Protection Policy (SEC-2025-001). I accept that failure to follow the mandatory verification steps may result in personal financial liability, termination, and legal consequences.

Name ________________________________ Employee ID ________________________________
Department____________________________Signature_________________________________
Date __________________________________