Deepfake Defense Policy

Protecting our organization from AI-generated impersonation threats

Purpose

To safeguard the company, employees, and clients from fraudulent use of deepfake audio, video, or images intended to deceive, mislead, or cause financial or reputational harm.

Scope

This policy applies to all employees, contractors, and stakeholders who may receive or act upon communications appearing to come from company leadership, clients, or partners.

Key Principles

- Verify Before Acting – No financial or sensitive action is taken based on a single channel of communication.
- Trust but Confirm – Always confirm identity through a secondary method.
- Be Aware – Recognize that deepfakes may look or sound authentic but contain small inconsistencies.

Verification Procedures

- Dual Approval: All financial transactions over $___ require at least two authorized sign-offs.
- Secondary Channel: Confirm requests through a different channel (phone call, secure chat, in-person) before proceeding.
- Passphrases: Executives and managers use internal verification codes/phrases for sensitive instructions.
- Suspicion Protocol: If a message seems unusual, urgent, or “out of character,” treat it as potentially fraudulent until verified.

Detection Awareness

- Lip movements slightly mismatched with speech.
- Unnatural eye blinking or facial expressions.
- Robotic or inconsistent voice tone.
- Urgent requests for money, access, or data.

Reporting

Immediately report suspected deepfake attempts to IT Security and Management. Do not delete suspicious files or messages—preserve evidence.

Technology Safeguards

- The company will evaluate and implement AI deepfake detection tools where practical.
- Regular monitoring of executive and brand likenesses online.
- Promotion of digital signatures or watermarking for official company content.

Disciplinary & Legal Response

Employees who fail to follow this policy may be subject to disciplinary action. Legal action will be taken against malicious actors when possible.

Reminder

Remember: If something feels off, pause and verify. It’s better to delay a transaction than to risk costly fraud.