DEEPFAKE DEFENSE POLICY

Organizational Framework for AI-Generated Fraud Prevention

EXECUTIVE ALERT: Deepfake technology enables sophisticated impersonation attacks targeting financial controls, identity verification, and trust-based processes. Threat actors can now convincingly replicate executive voices, video appearances, and behavioral patterns to authorize fraudulent transactions, manipulate HR systems, and bypass security controls. This policy establishes mandatory safeguards to protect organizational assets.

TOP 5 ORGANIZATIONAL DEFENSE CONTROLS

1. MULTI-CHANNEL VERIFICATION PROTOCOL

Policy: All high-risk requests (funds transfer >$10K, banking changes, credential resets, policy modifications) require verification through TWO independent channels with different communication methods.

- **Implementation:** Primary channel (email/video call) must be verified via secondary channel (phone callback to known number, in-person confirmation, or authenticated mobile app)
- **Department Ownership:** Finance (financial transactions), HR (personnel changes), IT (system access)
- **Tools:** Callback verification lists, secure authentication apps (Duo, Okta Verify), documented approval workflows
- **Timeline:** Deploy within 30 days | Priority: CRITICAL

2. ENHANCED MULTI-FACTOR AUTHENTICATION (MFA)

Policy: Mandatory phishing-resistant MFA for all financial systems, HR platforms, email, and privileged access. SMS-based authentication is explicitly PROHIBITED for sensitive operations.

- **Implementation:** Deploy hardware security keys (YubiKey, Titan) or biometric authentication for Tier 1 users (executives, finance, HR leadership)
- **Department Ownership:** IT Security with Finance/HR stakeholder approval
- **Tools:** FIDO2-compliant hardware keys, Windows Hello for Business, Touch ID/Face ID for mobile access
- **Timeline:** Phase 1 (Executives): 15 days | Phase 2 (All staff): 60 days | Priority: CRITICAL

3. DEEPFAKE AWARENESS TRAINING PROGRAM

Policy: Quarterly mandatory training on deepfake detection, social engineering tactics, and verification protocols. All employees handling financial/personnel data must complete deepfake simulation exercises.

- **Implementation:** Interactive training modules with real deepfake examples, simulated attack scenarios, red flags identification (audio artifacts, unnatural expressions, request urgency)
- **Department Ownership:** HR Learning & Development with IT Security consultation
- **Tools:** KnowBe4, Proofpoint Security Awareness, custom deepfake detection workshops
- **Timeline:** Initial training: 45 days | Quarterly refreshers | Priority: HIGH

4. AI-POWERED DETECTION & MONITORING

Policy: Deploy automated deepfake detection for voice communications, video conferencing, and email authentication. Real-time monitoring for anomalous financial transaction patterns and behavioral deviations.

- **Implementation:** Voice biometrics for high-value calls, video authentication watermarking, DMARC/SPF/DKIM email validation with advanced threat protection
- **Department Ownership:** IT Security / SOC with Finance approval for transaction monitoring rules
- **Tools:** Pindrop (voice authentication), Reality Defender, Microsoft Defender, Abnormal Security (email), SIEM correlation rules
- **Timeline:** Voice/video: 60 days | Email enhancement: 30 days | Priority: HIGH

5. CONTINUOUS AUDIT & INCIDENT RESPONSE

Policy: Weekly audit logs for all high-risk transactions, monthly control effectiveness reviews, and immediate incident response protocols for suspected deepfake attacks with forensic preservation.

- **Implementation:** Automated logging of verification attempts, failed MFA, unusual authorization patterns; dedicated deepfake incident playbook; quarterly red team exercises
- **Department Ownership:** Internal Audit with IT Security and Legal counsel
- **Tools:** Splunk/ELK Stack for log analysis, incident response platform (ServiceNow), forensic tools for media authentication
- **Timeline:** Logging infrastructure: 30 days | IR playbook: 15 days | Priority: CRITICAL

COMMON DEEPFAKE THREAT SCENARIOS

Icon	Threat Scenario	Attack Vector	Target Systems	Primary Defense
🎙	**CEO Voice Fraud**	AI-cloned executive voice authorizes urgent wire transfer via phone/voicemail	Banking systems, Finance approvers	Multi-channel callback verification, voice biometrics
📹	**Video Conference Impersonation**	Deepfake video of executive in Zoom/Teams approving policy changes or transactions	Virtual meetings, approval workflows	Pre-established codewords, out-of-band confirmation
❗	**Vendor Payment Redirect**	Cloned vendor contact requests bank account update via email + confirmation call	AP systems, vendor portals	Verification via original vendor contact, payment holds >48hrs
✉	**HR Banking Information Change**	Employee impersonation (voice + email) requests direct deposit account modification	HRIS, payroll systems	In-person verification or video call with ID presentation
✓	**Identity Verification Bypass**	Deepfake video used to pass KYC/identity checks for account opening or password resets	Customer onboarding, account recovery	Liveness detection, document verification, behavioral biometrics
🎙	**Helpdesk Social Engineering**	Voice-cloned executive calls IT helpdesk for urgent password reset or MFA removal	IT support systems, IAM platforms	Mandatory callback verification, no phone-only privileged changes
✉	**Attorney/Legal Impersonation**	Deepfake voice claiming to be legal counsel authorizing confidential data release or settlement payment	Legal holds, wire transfers, NDA processes	Direct contact with known legal counsel, legal dept approval required
📹	**Board/Investor Fraud**	Fake video of board member or investor requesting expedited capital distribution or strategic pivot	Board resolutions, investor relations	Formal board meeting protocols, written resolutions, legal review

IMMEDIATE ACTION ITEMS FOR LEADERSHIP:
✓ Approve emergency funding for phishing-resistant MFA deployment (30-day target)
✓ Designate Control Owners for each of the 5 defense controls above
✓ Schedule executive deepfake awareness briefing (next board meeting)
✓ Authorize IT Security to implement transaction verification protocols
✓ Review and update financial authorization thresholds and dual-approval requirements