Information Security Policy (ISP)

Effective Date: January 3, 2026

Review Cycle: Annual (Next Review: January 2027)

1. Purpose & Scope

The ISP defines the technical framework used to protect the Confidentiality, Integrity, and Availability (CIA) of data processed by OTG. This policy applies to all hardware, software, and network infrastructure located at the OTG Lahore facility.

2. Network Security (No-VPN / Static IP Model)

- **Static IP Whitelisting:** All outbound traffic to client environments is restricted to OTG's designated Static IP address. Clients are requested to whitelist this IP to prevent unauthorized access from outside our facility.
- **Firewall Management:** OTG utilizes a Next-Generation Firewall (NGFW) with Intrusion Prevention Systems (IPS) enabled. All non-essential ports (e.g., RDP, FTP) are closed by default.
- **Network Segmentation:** The operational floor network is physically or logically separated from the guest Wi-Fi and administrative networks.

3. Endpoint & Workstation Security

- **Standard Image:** All agent workstations run a "Locked Down" OS image. Users do not have Administrative Rights.
- **Encryption:** Every workstation uses **AES 256-bit** full-disk encryption (e.g., BitLocker).
- **Automatic Lock:** Screens are set to automatically lock after **3 minutes** of inactivity.
- **Endpoint Protection:** Managed Anti-Malware and Endpoint Detection and Response (EDR) software is installed on all machines, with definition updates pushed every 24 hours.

4. Identity & Access Management (IAM)

- **Principle of Least Privilege:** Access is granted only to the specific tools required for an agent's current shift/campaign.
- **Multi-Factor Authentication (MFA):** Mandatory MFA is required for all OTG internal systems (Email, HR portal, etc.). We encourage clients to enforce MFA on their platforms used by OTG agents.
- **Unique Credentials:** No "shared" or "generic" accounts are permitted. Every agent uses a unique, trackable ID.

5. The "Clean Desk" Technical Control

- **Peripheral Blocking:** USB ports on all agent workstations are software-disabled to prevent data exfiltration via thumb drives.
- **Shadow IT Blocking:** Access to personal email, cloud storage (Dropbox/Google Drive), and social media is blocked at the network level.

6. Monitoring & Auditing

- **Log Retention:** System logs (Logins, File Access, Network Traffic) are retained for **90 days** for forensic purposes.
- **Live Monitoring:** Supervisors utilize real-time screen monitoring software to ensure agents are adhering to security protocols.

7. Power & Connectivity Resilience

- **N+1 Redundancy:** To counter local utility instability, OTG maintains an Uninterruptible Power Supply (UPS) system and an on-site backup generator to ensure 99.9% uptime for global clients.