Professional Services & Staff Augmentation Security Requirements

Purpose

Professional Services firms and Staffing Agencies with access to Lucid Group, Inc. (“Lucid” or “Company”) and/or consumer Restricted, Confidential, or Internal Use Only data as defined within the Lucid Data Classification Standard (“Lucid Data”) or Lucid systems (“Systems”) must abide by these Professional Services/Staff Augmentation Security Requirements (“Security Requirements” or “Requirements”).

Scope

These Requirements apply to all Professional Services firms and Staffing Agencies (“Service Providers”) and the individuals assigned to perform services for Lucid (“Assigned Staff”).

Measure Category and Requirements

- Background Check
    - The Service Provider is required to provide third-party certified attestation of completed Assigned Staff background check findings within the past 12 months as a condition of engagement and physical or logical access to any Lucid asset. This requirement is mandatory and must comply with applicable laws and regulations. The background check must include Criminal Records, Credit verification (only applicable to Assigned Staff with access to financial data), Employment verification, Drug screening (only applicable to Assigned Staff with responsibility for driving or operating heavy machinery)
- Location of Resources
    - As a prerequisite for engagement, the Service Provider must disclose to the Company the intended physical location of Assigned Staff who are proposed to render services to Lucid. Additionally, if the Assigned Staff are expected to access Lucid Data from a different country or state due to a change in physical location or personal travel, the Service Provider must immediately inform the company.
- Lucid Acceptable Use Policy and Cybersecurity / Privacy Policies and Standards
    - Throughout the duration of the engagement and delivery of goods or services, the Assigned Staff must comply with the Company's Acceptable Use Policy, Cybersecurity, and Privacy Policies and Standards. Failure to do so will result in immediate termination of the Agreement.
- Lucid Approved Remote Access Mechanisms
    - Assigned Staff must comply with approved mechanisms for access to Lucid Systems and Data.
- Data Protection Requirements
    - Service Provider shall maintain at all times appropriate information security measures to protect the confidentiality, integrity, and availability of Lucid Data, including internationally recognized information security standards and technical and organizational measures.
- Incident Notification
    - Service Provider must, by confirmed delivery within 48 hours after becoming aware of a Security Breach (actual or reasonably suspected unauthorized access to, or disclosure or acquisition of Lucid Data), inform Company of the nature of the Security Breach, the likely consequences of the Security Breach, and the measures taken or proposed to be taken to address the Security Breach, and mitigate possible adverse effects.
- Subcontractors / Subprocessors
    - Service Provider must obtain written approval from the Company before engaging: (a) any subcontractors in the delivery of goods or services, or (b) third parties processing Lucid Data or accessing Lucid Systems. The Service Provider is responsible for developing, implementing, and executing a third-party security risk management program. This program should efficiently identify and manage cybersecurity risks associated with the use of third-party services or external (non-Lucid or non-Service Provider) systems. The Service Provider will promptly provide evidence of due diligence to Lucid, if requested.
- Security Audit Rights
    - During business hours and upon reasonable advance notice, Company and its agents may audit or otherwise assess Service Provider’s security, privacy, availability, confidentiality, and processing integrity controls,

policies, and procedures. Service Provider will facilitate, without delay, all reasonable and necessary access by Lucid and its agents to conduct and complete said assessment or audit.

- Engagement Conclusion
    - Service Provider must inform the Company in writing and within 12 hours of the completion of services provided or completion of Assigned Staff specific role or activities so that access to Lucid Systems and/or Lucid Data is appropriately terminated or modified.
- Offboarding
    - Service Provider is ultimately responsible for any badges and devices provided by Lucid including timely return of badges and devices at the conclusion of overall Engagement and / or conclusion of activities performed by Assigned Staff.