ESG@CoviaCorp.com

COVIA

CYBERSECURITY & DATA PRIVACY

We are committed to protecting our Team Members, assets, and operations from cyber-threats, and we proactively manage risks and performance in this area. We continue to invest in advanced security measures to protect our growing hybrid workforce, and we are focused on implementing additional automation tools to strengthen and streamline our remediation capabilities.

Approach

We rely on a comprehensive, multilayered defense strategy with robust cybersecurity standards and policies to mitigate security risks and foster consistency across our international security operations to bolster resilience against global threats.

Our efforts are focused on several critical areas, including:

- **Team Member Awareness** – Team Members are our first line of defense against potential threats, and we continue to take a proactive approach to cybersecurity awareness and readiness and prioritize user training and cybersecurity best practices. We conduct quarterly cybersecurity training and monthly phishing simulations.

  Our comprehensive cybersecurity training module is required for new Team Members during their onboarding process, and annually thereafter. Team Members in higher-risk roles are required to complete targeted training modules as well as tabletop risk simulations to practice threat response.

- **Technology Solutions** – All Covia systems utilize multi-factor authentication (MFA) requirements. Our advanced email filtering solutions reduce the quantity of phishing and malicious emails, and promptly detect and address these forms of threats. We routinely assess our tools and processes to improve our security posture.

- **Continuous Monitoring** – Our Security Operations Center monitors Covia systems 24/7/365 using comprehensive threat-identification mechanisms to ensure prompt and complete mitigation. We also conduct third-party penetration tests annually to detect and address potential vulnerabilities.

- **Incident Response** – We have developed detailed Incident Response Playbooks for various types of cyber breaches that document different technical and non-technical steps required for swift incident response. Regardless of breach type, steps are grouped into categories, such as: identification, notification, containment, eradication, recovery, and lessons learned.

- **Limited Data Access** – We adhere to the principle of least privilege with respect to data security. Under this principle, we grant access to the data we collect and share only with Team Members who require it to fulfill their job responsibilities.

CYBERSECURITY & DATA PRIVACY

- **Confidential Information** – We maintain appropriate administrative, technical, physical, and organizational safeguards designed to help protect personal or confidential data from unauthorized disclosure or access. Non-disclosure agreements (NDAs) are routinely executed with the appropriate stakeholders before sharing or receiving confidential information.

  We store personal data for no longer than is necessary for the performance of our obligations or to achieve the purposes for which the data was collected, as permitted under applicable law. To determine the appropriate retention period, we consider the amount, nature, and sensitivity of the data; the potential risk of harm from unauthorized use or disclosure of the data; the purposes for which we process the data and whether we can achieve those purposes through other means; and the applicable legal requirements. Unless otherwise required by applicable law, at the end of the retention period we remove personal data from our systems and records or take appropriate steps to properly anonymize it.

- **Whistleblower Procedures** – We maintain a confidential third-party Whistleblower Hotline, which is available 24/7 for reporting of information and system security concerns. Those submitting a complaint may choose to remain anonymous, and we conduct a thorough investigation, based on the severity of the submission, to determine the appropriate resolution.

2030 GOALS THAT INSPIRE:

Complete annual and continuous cybersecurity training by 100% of our Team Members.

SUPPORTING POLICIES:

- Code of Business Conduct & Ethics
- Acceptable Use Policy
- Online U.S. Privacy Policy
- EU Privacy Notice

CYBERSECURITY AND DATA PRIVACY OVERSIGHT

Our cybersecurity and data privacy program is monitored and overseen by the following:

Information Security Team

Develops and implements our cybersecurity strategy. Their primary goal is to safeguard the confidentiality, integrity, and availability of our data and systems.

↓

Compliance Team

Ensures that Covia complies with data protection laws and regulations, both locally and globally.

↓

Incident Response Team

Manages response and recovery efforts in the instance of a security breach or incident to minimize potential damage.