INFORMATION SECURITY PROGRAM MANAGEMENT

Cross Country Healthcare is committed to protecting its employees, partners, clients and Cross Country Healthcare from damaging acts that are intentional or unintentional. In achieving this goal, Cross Country Healthcare has an enterprise-level, Information Security program including policies, standards, controls, employee training and awareness, incident reporting, and reviews, that is geared towards mitigating the risk of loss and / or misuse of our critical information assets and helping prevent disruption of our business operations.

Cross Country Healthcare's Information Security program was created using guidelines from The National Institute of Standards and Technology (NIST) and is aligned to the NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations.

ORGANIZATION AND GOVERNANCE

Cross Country has a dedicated Director of Security, Risk, and Compliance who (along with other team members) is responsible for leading enterprise-wide information security strategy, policy, standards, and processes. The Director of Security, Risk, and Compliance is part of Cross Country Healthcare's Information Technology group and works across all business units within the company to protect Cross Country Healthcare, its brand, employees, consultants, and customers against cybersecurity risks.

Security governance also involves the Security and Privacy Steering Committee which represents Management's efforts to implement information security and privacy compliance programs that are aligned with company strategy and supportive of the organizations' Information Security and Privacy Policies. This committee meets on a quarterly basis and receives updates from the Director of Security, Risk, and Compliance, other members of the Cross Country leadership and operations teams, and other cybersecurity subject matter experts regarding current cybersecurity threats, cybersecurity technologies and solutions deployed and being planned, cyber risks and cybersecurity incidents; the committee is also involved in the approval process for policies and standards, and all security policies are ultimately approved by the Chief Executive Officer. The Security and Privacy Steering Committee provides periodic updates (at least every (6) six months) to the senior leadership of the company, the Audit Committee, and the Board of Directors.

PROGRAM OVERVIEW

Cross Country Healthcare is committed to protecting its employees, consultants, partners, clients and Cross Country Healthcare systems from damaging acts, whether intentional or unintentional. Effective information security and privacy is a team effort involving the participation and support of every Cross Country Healthcare user who interacts with data and systems. Therefore, all users need to be aware of all policies, standards, procedures, and guidelines, and to conduct their activities accordingly. This information, along with other critical security content is communicated to all employees and consultants as a part of our ongoing Security Awareness program.

The security of systems includes controls and safeguards to offset possible threats, as well as controls to ensure availability, integrity, and confidentiality of the data:

- **Confidentiality** – preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- **Integrity** – ensuring that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **Availability** – ensuring timely and reliable access to and use of information.

Security measures are taken to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes accidental loss or destruction.

POLICIES, STANDARDS, PROCEDURES & GUIDELINES

The Cross Country Information Security policy documentation addresses the following specific control areas:

- Security and Compliance Program Management
- Assessment, Authorization, and Monitoring Policy
- Security Planning
- Risk Assessment
- Awareness & Training
- Configuration Management
- Contingency Planning
- Incident Response
- Systems Maintenance
- Media Protection
- Personnel Security
- Physical & Environmental Protection
- System & Information Integrity
- Access Control
- Audit & Accountability
- Identification & Authentication
- System & Communication Protection
- Data Classification and Handling
- Supply Chain Risk Management