



## 01-Introduction to the Information Security Policy

Approved by: William Voss

Review: Annual

Renewed By:

Effective: April 1, 2024

Revised:

Renewed:

---

# Introduction to the Information Security Policy

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the confidentiality, integrity and availability of the data environment at River City TMS, PLLC, hereinafter, referred to as River City TMS, PLLC. It serves as a central policy document with which all workforce members and contractors must be familiar and defines actions and prohibitions that all users must follow.

### Scope

This policy encompasses common security requirements for all Organization personnel and systems that create, receive, maintain, or transmit electronic protected health information (ePHI). It also applies to information resources owned by others, such as contractors of River City TMS, PLLC, entities in the private sector, and in cases where River City TMS, PLLC has a legal, contractual or fiduciary duty to protect said resources while in Organization custody. In the event of a conflict, the more restrictive measures apply. This policy covers River City TMS, PLLC network system which is comprised of various hardware, software, communication equipment and other devices designed to assist River City TMS, PLLC in the creation, receipt, storage, processing, and transmission of ePHI. This definition includes equipment connected to any River City TMS, PLLC domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by River City TMS, PLLC at its office locations or at remote locales.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Organization workforce members or temporary workers at all locations and by contractors working with River City TMS, PLLC as subcontractors.

### Applicable Statutes / Regulations

The laws, mandates, and regulations of the U.S. Department of Health and Human Services were incorporated into the various policy statements included in this document to ensure appropriate



security management processes in accordance with security and privacy policies or state or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

U.S. Department of Health and Human Services

Health Information Privacy

<http://www.hhs.gov/ocr/privacy/index.html>

Each of the policies defined in this document is applicable to the task being performed, not just specific departments or job titles.

### **Privacy Officer (PO) [§164.530\(a\)\(1\)](#)**

River City TMS, PLLC has established a Privacy Officer as required by HIPAA. This Privacy Officer will oversee all ongoing activities related to the development, implementation (to include monitoring and communication), and maintenance of the Organization privacy policies in accordance with applicable federal and state laws. The current Privacy Officer for the Organization is:

- William D Voss 509-960-1671

### **Security Officer (SO) [§164.308\(a\)\(2\)](#)**

The Organization has established a Security Officer as required by HIPAA. This Security Officer will oversee all ongoing activities related to the development, implementation (to include monitoring and communication), and maintenance of River City TMS, PLLC security policies in accordance with applicable federal and state laws. The current Security Officer for River City TMS, PLLC is:

- Toni Barthell 509-960-1671

### **Risk Management Team (RMT)**

River City TMS, PLLC has established a Risk Management Team made up of key personnel whose responsibility it is to identify areas of concern within River City TMS, PLLC and to act as the first line of defense in enhancing the appropriate privacy and security posture.

All RMT members identified within this policy are assigned to their positions by the CEO/Owner, N/A. The term of each member assigned is at the discretion of the CEO/Owner, but generally it is expected that the term will be one year. Members for each year will be assigned at the first meeting of the Leadership Team in a new calendar year. This committee will consist of the positions within River City TMS, PLLC most responsible for the overall security policy planning of River City TMS, PLLC, which are the CEO/Owner (William David Voss), Operations Manager (Toni Barthell).