101 Tosca Drive
Stoughton, MA 02072 USA
(Phone) 781.297-2034
(FAX) 781.297-2039
(Web) www.csmisolutions.com

# SportsWareOnLine Security Statement

This document describes CSMi's SportsWareOnLine security procedures.

## Microsoft Azure Hosting

1. The SportsWareOnLine application and data files are hosted in the Microsoft Azure environment. A current list of the Azure compliance certifications is available at: https://docs.microsoft.com/en-us/azure/compliance/

The following information details additional CSMi procedures and practices.

## HIPAA/FERPA

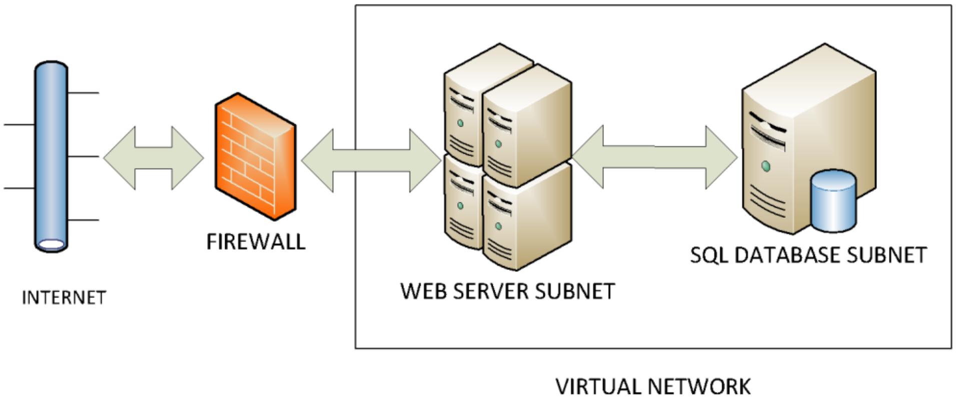
1. CSMi's procedures, our SportsWareOnLine product, and our website hosting are HIPAA and FERPA compliant.
2. Criminal background checks are run on all CSMi employees with access to PHI.
3. Employees with access to ePHI undergo annual HIPAA training.

## GDPR

1. CSMi's GDPR statement can be downloaded from: https://sportswareonline.com/SWOL_Downloads/200349_CSMi_GDPR_Statement.pdf

## Network Topology

1. The environment consists of a Web server and an SQL server separated into two segregated subnets. Each subnet is protected by an Azure Network Security Group (NSG) which acts as a firewall, only allowing traffic explicitly allowed in the NSG rules.
2. The SQL Server does not have a public IP address.
3. The Web Application Firewall detects suspicious traffic.
4. The following diagram illustrates the hosting network topology.



## Encryption

1. All data at rest is encrypted with AES-256 encryption.

## Replication

1. The SWOL data is replicated to three separate drive pieces of hardware to ensure data durability. If one or even two replicas experience issues, the remaining replicas help ensure persistence of the SWOL data and high tolerance against failures.

## Domestic Hosting

1. All data is hosted within the US.

## Data Backup

1. Daily backup with a 30-day retention policy.

## Anti-Virus Updates/OS Patches

1. Trend Micro Anti-Virus, Host Intrusion Prevention System (HIPS), and File Integrity Monitoring.
2. Azure DDoS protection.
3. QRadar Security Operations Center (SOC) services. Sumo Logic SIEM (Security Information and Event Management) program. UEBA (user and entity behavior analytics).
4. Monthly OS patching.
5. Security Operation Center (SOC) monitoring 24/7/365.

## Reporting

1. Weekly intrusion prevention reports.
2. Monthly server vulnerability scanning.

## Software Release Process

1. Code Development is performed on local CSMi machines.

2. Code is released to an internal CSMi server for testing by different CSMi developers.
3. Upon acceptance on the internal server, code is released to a test site for QA testing by CSMi and select customers.
4. Upon acceptance on the test server, the code is released to the live site.