Office of the Chief Information Officer Directive: IT 5.03	Published: 02/2020
Chapter: Data Management	Last Review: 02/2024
Subject: **Management of Third-Party Services**	

1 DIRECTIVE

1.01 All contracts and Service Level Agreements (SLAs) with a third-party service (TPS) provider must include provisions for data management best practices including:

(a) Data processing integrity and validation.

(b) Data backup, both local and offsite.

(c) Data security and confidentiality corresponding to company-specified data classifications.

(d) Data encryption for all data transmissions across potentially hostile environments such as the Internet.

(e) Data exchange compatibility with company systems and applications.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that all company policies for internal data management are adhered to and no control exposures are created using a TPS provider.

3 SCOPE

3.01 This directive applies to all employees who negotiate contracts and SLAs with TPS providers or receive services from a TPS provider, and to IT Senior Leadership.

4 RESPONSIBILITY

4.01 All managers who plan outsourced IT production, create requirements for TPS providers or negotiate contracts or SLAs with TPS must ensure that specifications and agreements include compliance with all company policies with respect to data management.

5 DEFINITIONS

5.01 "**Service Level Agreement**" **(SLA)** is part of the contract where the service level to be provided is defined. It usually includes such elements as uptime, response time or delivery time, probable volumes, etc.

5.02 "**Third Party Service**" **(TPS)** is an external company providing outsourced services. For IT, this may also be referred to as an outsourcing service provider. In the context of data management, a TPS may provide services including any of: offsite storage of data, data entry, auxiliary data processing or even completely contained data processing managing a company's data in its entirety.

6 RELATED DIRECTIVES

OCIO IT 5.01 – Data Processing Integrity and Validation
OCIO IT 5.02 – Data Backup and Storage
OCIO IT 5.07 – Anti-Spam Requirements
OCIO IT 8.01 – Physical and Infrastructure Security
OCIO IT 8.02 – Systems Security
OCIO IT 8.04 – Confidentiality and Privacy
OCIO IT 9.02 – Data Classification
OCIO IT 9.03 – Data Access Controls
OCIO IT 9.04 – Application Security Controls
OCIO IT 9.05 – Data Disposal