



Finance and Administrative Services Department

Enterprise Technology Services Division

1 North University Drive, Suite 4003A • Plantation, Florida 33324-2019 • 954-357-6512 • FAX 954-357-5601

MEMORANDUM

TO: Brenda Billingsley, Director, Purchasing

FROM: Benjamin Sanchez, Information Systems Administrator, Enterprise Technology Services

DATE: April 27, 2020 BENJAMIN SANCHEZ Digitally signed by BENJAMIN SANCHEZ
Date: 2020.04.27 17:46:47 -04'00'

SUBJECT: Splunk Log Management and Security Information and Event Management (SIEM) System – Request for Standardization

ETS requests approval for standardization for the Splunk Log Management and SIEM system. Splunk provides a central repository for collecting and monitoring data from multiple systems and applications across Broward County. Additionally, Splunk provides:

- Real-time visibility across the County's information security systems
- Seamless integration with the following County systems:
 - Cloud Enterprise Resource Planning (ERP) system - PeopleSoft
 - Windows servers
 - Firewalls and security systems
 - Databases
 - Applications
- Event log management that consolidates data from numerous sources
- A correlation of events gathered from different logs or security sources, using logic rules that add intelligence to raw data, and
- Automatic security event notifications and visualized dashboards for investigating security issues
- Faster response and triage of security incidents

As the County's primary security monitoring and alerting system, Splunk has identified multiple security threats across the County network. This solution has been integrated with the County's ERP system at implementation of PeopleSoft.

Splunk has proven to be compatible within the County's network infrastructure and systems. Splunk offers a cost effective and flexible way to meet compliance requirements including audit trail collection, monitoring, and reporting into a single solution to help assess the County's security profile. It provides consistency for operational support, and satisfies regulatory and industry log management standards such as Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI).