Security Requirements

The following requirements are applicable to the Contract:

Employee Identification

A. Contractor Personnel shall display his or her company ID badge in a visible location at all times while on Erie County premises. Upon request of authorized County personnel, each Contractor Personnel shall provide additional photo identification.
B. Contractor Personnel shall cooperate with County site requirements, including but not limited to, being prepared to be escorted at all times, and providing information for County badge issuance.

Security Clearance / Criminal Background Check

A. A criminal background check for any Contractor Personnel shall be completed prior to each Contractor Personnel providing any services under the Contract.
B. The Contractor shall provide certification to the Department that the Contractor has completed the required criminal background check described in this RFP for each required Contractor Personnel prior to assignment, and that the Contractor Personnel have successfully passed this check.

Information Technology

A. All Contractors shall comply with and adhere to the County IT Security Policy and Standards. These policies may be revised from time to time and the Contractor shall comply with all such revisions. Updated and revised versions of county IT Policy and Standards. **keyword: Security Policy.**
B. All Contractor shall not connect any of its own equipment to a County LAN/WAN without prior written approval by DISS. The Contractor shall complete any necessary paperwork as directed and coordinated with DISS to obtain approval to connect Contractor owned equipment to the county LAN/WAN.

The Contractor shall:

I. Implement administrative, physical, and technical safeguards to protect county data that are no less rigorous than accepted industry best practices for information security.
II. Ensure that all such safeguards, including the manner in which county data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws as well as the terms and conditions of the contract.
III. The Contractor, and Contractor Personnel, shall:
    a. Abide by all applicable federal, State, and local laws, rules and regulations concerning security of Information Systems and Information Technology
    b. Comply with and adhere to the County IT Security Policy and Standards as each may be amended or revised from time to time.

Data Protection and Controls

Contractor shall ensure a secure environment for all county data and any hardware and software (including but not limited to servers, network, and data components) provided or used in connection with the performance of the Contract and apply appropriate controls to maintain a secure environment (“Security Best Practices”). Such Security Best Practices shall comply with accepted industry standard, such as the NIST cybersecurity framework.

Security Logs and Reports Access

For a SaaS or non-county hosted solution, the Contractor shall provide reports to the county in a mutually agreeable format.

Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all county files related to the Contract.

PCI Compliance

Contractor shall at all times comply, and ensure compliance with, all applicable Payment Card Industry ("PCI") Data Security Standards (“DSS”), including any and all changes thereto. Contractor shall provide the county with documented evidence of current compliance to PCI DSS within 30 days of the request.

The Contractor shall annually furnish to the county, evidence of the PCI Security Standards Council’s (SSC) acceptance or attestation of the Contractor’s conformance to the relevant PCI DSS requirements by a third party certified to perform compliance assessments.

The Contractor shall ensure that the scope of the annual SOC 2 Type II Report includes testing to confirm the PCI assessment results.

Security Incident Response

The Contractor shall notify the County when any Contractor system that may access, process, or store county data or county systems experiences a Security Incident, or a Data Breach.

Notify the County within twenty-four (24) hours of the discovery of a Security Incident by providing notice via written or electronic correspondence to DISS, chief information officer and chief information security officer.

SOC 2 Type 2 Audit Report

A SOC 2 Type 2 Audit applies to the Contract. The applicable trust services criteria are Security, Availability, Processing Integrity, Confidentiality, or Privacy

The Contractor shall have an annual audit performed by an independent audit firm of the Contractor’s handling of Sensitive Data and/or the Department’s critical functions. Critical functions are identified as all aspects and functionality of the System including any add-on

modules and shall address all areas relating to Information Technology security and operational processes. These services provided by the Contractor that shall be covered by the audit will collectively be referred to as the "Information Functions and/or Processes." Such audits shall be performed in accordance with audit guidance: Reporting on Controls at a Service Organization Relevant to Security, Availability, Confidentiality, or Privacy (SOC 2) as published by the American Institute of Certified Public Accountants (AICPA) and as updated from time to time, or according to the most current audit guidance promulgated by the AICPA or similarly-recognized professional organization, as agreed to by the Department, to assess the security of outsourced client functions or data (collectively, the "Guidance") as follows:

A. The type of audit to be performed in accordance with the Guidance is a SOC 2 Type 2 Audit (referred to as the "SOC 2 Audit" or "SOC 2 Report"). The initial SOC 2 audit shall be scheduled and completed within a timeframe to be specified by the county and submitted to DISS. All subsequent SOC 2 audits that are arranged after this initial audit shall be performed on an annual basis and submitted to DISS by the recurring annual date" for the preceding calendar year.
B. The audit scope of each year's SOC 2 Report may need to be adjusted (including the inclusion or omission of the relevant trust services principles of Security, Availability, Confidentiality, and Privacy) to accommodate any changes to the Contractor's environment since the last SOC 2 Report. Such changes may include but are not limited to the addition of Information Functions and/or Processes through modifications to the TO Agreement or due to changes in Information Technology or operational infrastructure implemented by the Contractor. The Contractor shall ensure that the audit scope of each year's SOC 2 Report engagement shall accommodate these changes by including in the SOC 2 Report all appropriate controls related to the current environment supporting the Information Functions and/or Processes, including those controls required by the TO Agreement.
C. The scope of the SOC 2 Report shall include work performed by any relevant subcontractors that provide essential support to the Contractor and/or essential support to the Information Functions and/or Processes provided to the Department under the TO Agreement. The Contractor shall ensure the audit includes all such subcontractor(s) operating in the performance of the TO Agreement.