

## **Enterprise Technology Services Security Requirements Exhibit – High Risk**

### **1. Definitions**

1.1. County Confidential Information means any County Data that includes employee information, financial information, protected health information, or personally identifiable information for individuals or entities interacting with County (including, without limitation, social security numbers, an individual's biometrics and geolocation, birth dates, banking and financial information, and other information deemed exempt or confidential under state or federal law or applicable regulatory body, including without limitation Section 501.171, Florida Statutes).

1.2. County Data means the data and information (including text, pictures, sound, graphics, video and other data) relating to County or its employees or subcontractors and any third parties, or made available or provided by County or its subcontractors and any third parties to Contractor, for or in the performance of this Agreement, including all derivative data and results derived therefrom, whether or not derived through the use of the Contractor's services, whether or not electronically retained, and regardless of the retention media.

1.3. Equipment means the hardware being provided by Contractor under the Agreement.

1.4. Software means software provided or licensed by Contractor pursuant to the Agreement.

All other capitalized terms not expressly defined within this exhibit shall retain the meaning ascribed to such terms in the Agreement (and if not so defined, then the plain language meaning appropriate to the context in which it is used).

### **2. County Network Access**

2.1. County Network Access. If Contractor will have access to any aspect of County's network via an Active Directory account, onsite access, remote access, or otherwise, Contractor must:

2.1.1. comply at all times with all applicable County access and security standards, regulatory requirements, policies, and procedures related to County's network, as well as any other or additional restrictions or standards for which County provides written notice to Contractor;

2.1.2. provide any and all information that County may reasonably request in order to determine appropriate security and network access restrictions and verify Contractor's compliance with County security standards;

2.1.3. provide privacy and cybersecurity training to its employees with access to County's network upon hire and at least once annually; and

2.1.4. notify County of any terminations or separations of Contractor's employees who had access to County's network.

In addition, for any remote access to County's network, Contractor must:

2.1.5. utilize secure, strictly-controlled industry standards for encryption (e.g., Virtual Private Networks, Multi-Factor Authentication (MFA), passphrases), and safeguard County Data that resides in or transits through Contractor's internal network from unauthorized access and disclosure;

2.1.6. utilize only connections that are under Contractor's complete control or under the complete control of a person or entity authorized in advance by County in writing; unencrypted third-party public WiFi networks are not permitted to be used to connect to County's network; ·

2.1.7. utilize only equipment that contains antivirus protection software with current signatures, a currently supported and fully patched operating system, firmware, and third-party applications that are configured for least privileged access;

2.1.8. utilize, at a minimum, industry standard security measures, as determined in County's sole discretion, to safeguard County Data that resides in or transits through Contractor's internal network from unauthorized access and disclosure; and

2.1.9. activate remote access from Contractor and its approved Subcontractors into the County network only to the extent necessary to perform Services under this Agreement, deactivating such access immediately after use.

If at any point in time County, in the sole discretion of its Chief Information Officer (CIO), determines that Contractor's access to any aspect of County's network presents an unacceptable security risk, or if Contractor exceeds the scope of access required to perform the required Services under the Agreement, County may immediately suspend or terminate Contractor's access and, if the risk is not promptly resolved to the reasonable satisfaction of the County's CIO, may terminate this Agreement or any applicable Work Authorization upon ten (10) business days' notice (including, without limitation, without restoring any access to County network to Contractor).

### 3. Data and Privacy

Data and Privacy. To the extent applicable to the Services being provided by Contractor under the Agreement, Contractor shall comply with all applicable data and privacy laws and regulations, including without limitation Florida Statutes Section 501.171 and Chapter 119, and shall ensure that County Data processed, transmitted, or stored by Contractor or in Contractor's system is not accessed, transmitted or stored outside the United States. Contractor shall not sell, market, publicize, distribute, or otherwise make available to any third party any personal identification or cybersecurity incident information (as defined by Florida Statutes Sections 501.171, 817.568,

or 817.5685, or Chapter 119, as amended) that Contractor may receive or otherwise have access to in connection with this Agreement, unless expressly authorized in advance by County. If applicable and requested by County, Contractor shall ensure that all hard drives or other storage devices and media that contained County Data have been wiped in accordance with the then-current best industry practices, including without limitation DOD 5220.22-M, and that an appropriate data wipe certification is provided to the satisfaction of the Contract Administrator.

#### 4. Cybersecurity Incidents

Cybersecurity Incidents. Contractor shall report any cybersecurity incident or random incident (as those terms are defined in Section 282.0041, Florida Statutes) impacting or relating to County Data (including but not limited to servers or fail-over servers) to County, including the details required by Section 282.3185(5)(a), in sufficient time to reasonably permit County to timely comply with any required reporting under Section 282.3185(b) and no later than twenty-four (24) hours after becoming aware of such breach (or such shorter time period as may be required under applicable law), unless an extension is granted by County's CIO. Contractor shall provide County with a detailed incident report within five (5) days after becoming aware of the breach, including remedial measures instituted and any law enforcement involvement. Contractor shall fully cooperate with County on incident response, forensics, and investigations into Contractor's infrastructure as it relates to any County Data or County applications.

#### 5. Managed or Professional Services

5.1. Managed or Professional Services. To the extent applicable to the Services being provided by Contractor under the Agreement:

5.1.1. Contractor shall ensure adequate background checks have been performed on any personnel having access to County Confidential Information. Contractor shall not knowingly allow convicted felons or other persons deemed by Contractor to be a security risk to access County Confidential Data. Contractor shall immediately notify County of any terminations or separations of Contractor's employees who performed Services under the Agreement and who had access to County Confidential Information or the County network.

5.1.2. Contractor shall not release County Data or copies of County Data without the advance written consent of County. If Contractor will be transmitting County Data, Contractor agrees that it will only transmit or exchange County Data via a secure method, including HTTPS, SFTP, or another method approved by County's CIO.

5.1.3. Contractor shall ensure the use of any open source or third-party software or hardware does not undermine the security posture of the Contractor or County.

## 6. System and Organization Controls (SOC) Report

System and Organization Controls (SOC) Report. If requested by County, Contractor must provide County with a copy of a current unqualified System and Organization Controls (SOC) 2 Type II Report for Contractor and for any third party that provides the applicable services comprising the system, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy), or a sworn declaration certifying Contractor has obtained the referenced SOC 2 Type II Report and listing all complementary user entity controls (CEUCs) identified therein, prior to commencement of the Agreement and on an annual basis during the Agreement, unless this requirement is waived or substitute documentation is accepted in writing by the County's CIO or designee.

## 7. Software Installed in County's Network

7.1. Software Installed in County's Network. To the extent Contractor provides any Software to be installed in County's network, Contractor must:

7.1.1. advise County of all versions of any third-party software (e.g., Java, Adobe Reader) to be installed and support updates for critical and high-risk vulnerabilities discovered in applicable third-party or open source software;

7.1.2. ensure that the Software is developed based on industry standards and best practices, including following secure programming techniques and incorporating security throughout the Software-development life cycle;

7.1.3. develop and maintain the Software to operate on County-supported and approved operating systems and firmware versions;

7.1.4. mitigate critical and high-risk vulnerabilities (as defined by Common Vulnerability and Exposures (CVE) scoring system) to the Software or Contractor platform within 30 days after patch release, and medium-risk vulnerabilities within 60 days after patch release, notifying County of proposed mitigation steps to be taken and timeline for resolution if Contractor is unable to apply a patch to remedy the vulnerability;

7.1.5. ensure the Software provides for role-based access controls and runs with least privilege access, enables auditing by default for any privileged access or changes, and supports electronic delivery of digitally signed upgrades from Contractor's or the third-party licensor's website;

7.1.6. ensure software connectivity to database systems can be configured to integrate with Active Directory (AD);

7.1.7. ensure the Software is not within three (3) years from its end-of-life date and provide County with end-of-life-schedules for all applicable Software;

7.1.8. support encryption using at a minimum Advanced Encryption Standard 256-bit encryption keys (“AES-256”) or current industry security standards, whichever is higher, for County Confidential Data at rest and use transport layer security (TLS) 1.2 or current industry standards, whichever is higher, for data in motion; and

7.1.9. upon request by County, provide an attestation letter identifying date of the most recent security vulnerability testing performed and any vulnerabilities identified and mitigated (must be dated within six (6) months after any major release).

## 8. Equipment Leased or Purchased from Contractor

8.1. Equipment Leased or Purchased from Contractor. To the extent Contractor is the Original Equipment Manufacturer (OEM) or an authorized reseller for the OEM for any Equipment provided under this Agreement, Contractor must:

8.1.1. ensure that physical security features to prevent tampering are included in any Equipment provided to County and ensure, at a minimum, industry-standard security measures are followed during the manufacture of the Equipment;

8.1.2. ensure any Equipment provided does not contain any embedded remote-control features unless approved in writing by County’s Contract Administrator, and disclose any default accounts or backdoors that exist for access to County’s network;

8.1.3. shall supply a patch, firmware update, or workaround approved in writing by County’s Contract Administrator within thirty (30) days after identification of a new critical or high risk vulnerability, and within sixty (60) days after identification of a medium risk vulnerability and notify County of proposed mitigation steps taken;

8.1.4. develop and maintain Equipment to interface with County-supported and approved operating systems and firmware versions;

8.1.5. upon request by County, make available any required certifications as may be applicable per compliance and regulatory requirements (e.g., Common Criteria, Federal Information Processing Standard 140);

8.1.6. ensure the Equipment is not within three (3) years from its end-of-life date at the time of delivery and provide County with end-of-life-schedules for all applicable Equipment;

8.1.7. (for OEMs only) support electronic delivery of digitally signed upgrades of any applicable Equipment firmware from Contractor’s or the OEM’s website; and

8.1.8. (for OEMs only) upon request by County, provide an attestation letter identifying date of the most recent security vulnerability testing performed and any vulnerabilities identified and mitigated (must be dated within six (6) months after any major release).

## 9. Payment Card Industry (PCI) Compliance

9.1. Payment Card Industry (PCI) Compliance. If and to the extent at any point during the Agreement the Software accepts, transmits, or stores any cardholder data or is reasonably determined by County to potentially impact the security of County's cardholder data environment ("CDE"), Contractor must:

9.1.1. comply with the most recent version of VISA Cardholder Information Security Program ("CISP") Payment Application Best Practices and Audit Procedures including Security Standards Council's Payment Card Industry ("PCI") Data Security Standard ("DSS"), including the functions relating to storing, processing, and transmitting of the cardholder data;

9.1.2. maintain PCI DSS compliance for the duration of the Agreement;

9.1.3. prior to commencement of the Agreement (or at such time the Software will process cardholder data), prior to Final Acceptance (if applicable), after any significant change to the CDE, and annually, provide to County: (i) a copy of Contractor's Annual PCI DSS Attestation of Compliance ("AOC"); and (ii) a written acknowledgement of responsibility for the security of cardholder data Contractor possesses or otherwise stores, processes, or transmits and for any service Contractor provides that could impact the security of County's CDE (if Contractor subcontracts or in any way outsources the credit card processing, or provides an API that redirects or transmits cardholder to a payment gateway, Contractor is responsible for maintaining PCI compliance for the API and providing the AOC for the subcontractor or payment gateway to County);

9.1.4. maintain and provide to County a PCI DSS responsibility matrix that outlines the exact PCI DSS controls that are the responsibility of either party and the PCI DSS controls that are the shared responsibility of Contractor and County;

9.1.5. follow Open Web Application Security Project (OWASP) for secure coding and transmission of cardholder data only to the extent Contractor provides a payment application;

9.1.6. immediately notify County if Contractor learns or suspects that Contractor, its Software, or its platform is no longer PCI DSS compliant and provide County the steps being taken to remediate the noncompliant status no later than seven (7) calendar days after Contractor learns or suspects it is no longer PCI DSS compliant;

9.1.7. activate remote access from Contractor and its approved Subcontractors into County's network only to the extent necessary to perform Services under this Agreement, deactivating such access immediately after use; and

9.1.8. maintain all inbound and outbound connections to County's CDE using Transport Layer Security (TLS) 1.2 or current industry standard, whichever is higher.

## 10. HIPAA Compliance

HIPAA Compliance. County has access to protected health information (“PHI”) that is subject to the requirements of 45 C.F.R. Parts 160, 162, and 164 and related regulations. If Contractor is considered by County to be a covered entity or business associate or is required to comply with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) or the Health Information Technology for Economic and Clinical Health Act (“HITECH”), Contractor shall fully protect individually identifiable health information as required by HIPAA or HITECH and, if requested by County, shall execute a Business Associate Agreement in the form set forth at [www.broward.org/Purchasing/Pages/StandardTerms.aspx](http://www.broward.org/Purchasing/Pages/StandardTerms.aspx). The County Administrator is authorized to execute a Business Associate Agreement on behalf of County. Where required, Contractor shall handle and secure such PHI in compliance with HIPAA, HITECH, and related regulations and, if required by HIPAA, HITECH, or other Applicable Law, include in its “Notice of Privacy Practices” notice of Contractor’s and County’s uses of client’s PHI. The requirement to comply with this provision, HIPAA, and HITECH shall survive the expiration or earlier termination of this Agreement. Contractor shall ensure that the requirements of this section are included in all agreements with Subcontractors.

## 11. Application Development Services

Application Development Services. To the extent applicable to the Services being provided by Contractor under the Agreement, Contractor shall develop, implement, and comply with industry-standard secure coding best practices as outlined by the County’s Service Provider Application Secure Coding Standard. In addition, if application development services are performed by Contractor augmented staff on behalf of County, staff must strictly follow and adhere to the County’s established application development policies, process, procedures, practices and standards. Upon request by County, Contractor shall provide an attestation letter to certify that security testing as specified above was performed along with security scan test results and tests performed. Any exceptions must be documented with the delivery of the attestation letter for acceptance by the County.