THIRD AMENDMENT TO SOFTWARE LICENSE AGREEMENT BETWEEN BROWARD COUNTY AND PIONEER TECHNOLOGY GROUP, LLC

This Third Amendment ("Third Amendment") to the Software License Agreement Between Broward County and Pioneer Technology Group, LLC is entered into by and between Broward County, a political subdivision of the State of Florida ("County"), and Pioneer Technology Group, LLC, a Florida limited liability company ("Contractor") (collectively County and Contractor are referenced as the "Parties").

RECITALS

A. The Parties entered into the Software License Agreement Between Broward County and Pioneer Technology Group, LLC, dated June 27, 2006, for Contractor's AXIA software, and a First Amendment, dated December 31, 2007, to amend pricing, and a Second Amendment, dated February 4, 2014, to extend the term and provide pricing (as amended, the "Agreement").

B. The current term for maintenance support services ("Maintenance" as defined in the Agreement) has been effectively extended through March 31, 2019.

C. The Parties wish to amend the Agreement to further extend the term, include additional pricing, and modify other provisions of the Agreement.

Now, therefore, for good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, County and Contractor agree as follows:

1. The above Recitals are true and correct and are incorporated herein by reference. All capitalized terms not expressly defined within this Third Amendment shall retain the meaning ascribed to such terms in the Agreement.

2. Except as modified herein, all terms and conditions of the Agreement remain in full force and effect. Amendments are indicated herein by use of strikethroughs to indicate deletions and bold/underlining to indicate additions.

3. The Parties acknowledge that County effectively extended Maintenance through March 31, 2019.

4. Sections 4.1 and 4.2 of the Agreement are replaced in their entirety with the following (bold/underlining omitted):

4.1 Public Records. To the extent Contractor is acting on behalf of County as stated in Section 119.0701, Florida Statutes, Contractor shall:

a) Keep and maintain public records required by County to perform the services under this Agreement;

b) Upon request from County, provide County with a copy of the requested records or allow the records to be inspected or copied within a reasonable time and at a cost that does not exceed that provided in Chapter 119, Florida Statutes, or as otherwise provided by law;

c) Ensure that public records that are exempt or confidential and exempt from public record requirements are not disclosed except as authorized by law for the duration of this Agreement and following completion or termination of this Agreement if the records are not transferred to County; and

d) Upon completion or termination of this Agreement, transfer to County, at no cost, all public records in possession of Contractor or keep and maintain public records required by County to perform the services. If Contractor transfers the records to County, Contractor shall destroy any duplicate public records that are exempt or confidential and exempt. If Contractor keeps and maintains the public records, Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to County upon request in a format that is compatible with the information technology systems of County.

A request for public records regarding this Agreement must be made directly to County, who will be responsible for responding to any such public records requests. Contractor will provide any requested records to County to enable County to respond to the public records request.

IF CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (954) 357-5961, VAB@BROWARD.ORG, 115 S. ANDREWS AVE., SUITE 120, FORT LAUDERDALE, FLORIDA 33301.

4.2 Trade Secret Materials. Any material submitted to County that Contractor contends constitutes or contains trade secrets or is otherwise exempt from production under Florida public records laws (including Chapter 119, Florida Statutes) ("Trade Secret Materials") must be separately submitted and conspicuously labeled "EXEMPT FROM PUBLIC RECORD PRODUCTION – TRADE SECRET." In addition, Contractor must, simultaneous with the submission of any Trade Secret Materials, provide a sworn affidavit from a person with personal knowledge attesting that the Trade Secret Materials constitute trade secrets under Section 812.081, Florida Statutes, and stating the factual basis for same. In the event that a third party submits a request to County for records designated by Contractor as Trade Secret Materials, County shall refrain from disclosing the Trade Secret Materials, unless otherwise ordered by a court of competent jurisdiction

or authorized in writing by Contractor. Contractor shall indemnify and defend County and its employees and agents from any and all claims, causes of action, losses, fines, penalties, damages, judgments and liabilities of any kind, including attorneys' fees, litigation expenses, and court costs, relating to the nondisclosure of any Trade Secret Materials in response to a records request by a third party.

5. The Agreement is amended to create Sections 6.5 and 6.6 as follows (bold/underlining omitted):

6.5 Compliance with Laws. Contractor shall ensure that the Licensed Software is fully accessible and compliant with the American with Disabilities Act, 42 U.S.C. § 12101, et seq., Section 504 of the Rehabilitation Act of 1973, and any related federal, state, or local laws, rules, and regulations, including as any of the foregoing may be amended from time to time, and that the Licensed Software meets or exceeds the World Wide Web Consortium/Web Content Accessibility Guidelines (WCAG) 2.0 Level AA standard or any higher standard as may be adopted by the International Organization for Standardization. Upon request by Contract Administrator, Contractor will provide County with any accessibility testing results and written documentation verifying accessibility, as well as promptly respond to and resolve any accessibility complaints.

6.6 Public Entity Crime Act; Discriminatory Vendors; Scrutinized Companies. Contractor represents that entry into this Agreement will not violate the Public Entity Crime Act, Section 287.133, Florida Statutes. Contractor further represents that there has been no determination that it committed a "public entity crime" as defined by Section 287.133, Florida Statutes, and that it has not been formally charged with committing an act defined as a "public entity crime" regardless of the amount of money involved or whether Contractor has been placed on the convicted vendor list. Contractor represents that it has not been placed on the discriminatory vendor list as provided in Section 287.134, Florida Statutes. Contractor further represents that it is not ineligible to contract with County on any of the grounds stated in Section 287.135, Florida Statutes.

6. Section 7.2 of the Agreement is amended as follows:

7.2 Commencement of Maintenance. Eighteen (18) months of Maintenance (the "Initial Term"), commencing upon County's Final Acceptance of the System, is included in the Software License for no additional fee, pursuant to the terms of Exhibit "C", Maintenance Support Services, concurrent to the Warranty period. Contractor agrees to provide up to five (5) additional years of Maintenance under this License Agreement, which annual term shall commence upon the expiration of the Initial Term. After the Initial Term, Contractor agrees to offer Maintenance to COUNTY as provided in Exhibit C hereto, ~~on an annual renewal basis~~ **as set forth herein**.

The "Anniversary Date" for the Annual Maintenance Charge shall be the first day after the expiration of the Initial Term. ~~The Annual Maintenance Charge for any additional~~

~~software licensed and installed after COUNTY finally accepts the System, will be listed on an amendment to Exhibit "C" and/or this License Agreement and shall be prorated to the next Anniversary Date, and thereafter, Maintenance will be invoiced at its Annual Maintenance Charge.~~

~~By the Second Amendment to the Agreement, the parties agree that the fifth year of Maintenance shall automatically extend through February 28, 2014 ("Initial Maintenance Term"), at no additional cost to County. Following the Initial Maintenance Term, the next year of Maintenance shall commence on March 1, 2014 and continue for thirteen months through and including March 31, 2015 ("Year Six").~~ Each year of Maintenance ~~after Year Six~~ will commence on April 1 and continue through March 31. ~~Upon the expiration of the Initial Maintenance Term,~~ Contractor shall provide ~~three additional (3) years of~~ Maintenance through and including March 31, 2017. Thereafter, County may extend the Maintenance for up to two (2) additional one-year renewal terms by providing written notice of renewal from the County's Purchasing Director at least ninety (90) days prior to the expiration of the then-current term. **Thereafter, County may extend the Maintenance for up to three (3) additional five-year renewal terms by providing written notice of renewal from the County's Purchasing Director at least ninety (90) days prior to the expiration of the then-current term.**

7. Section 7.6 of the Agreement amended as follows:

7.6 The **annual** cost for Maintenance ~~for each one (1) year term~~ after the Initial Term ("Annual Maintenance Charge") will be Thirty Seven Thousand Dollars ($37,000.00), which shall be prepaid annually.

8. Section 12.17 of the Agreement is amended and replaced in its entirety with the following (bold/underlining omitted):

12.17 Security; Access. Any access by Contractor to any aspect of the County's network must comply at all times with all applicable County access and security standards, as well as any other or additional restrictions or standards for which County provides written notice to Contractor. Contractor will 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. If at any point in time County, in the sole discretion of its Chief Information Officer, determines that Contractor's access to any aspect of the County's network presents an unacceptable security risk, 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 Chief Information Officer, may terminate this Agreement or any applicable Work Authorization upon ten (10) business days' notice (including, without limitation, without restoring any access to the County network to Contractor).

Any remote access by Contractor must be secure and strictly controlled with current industry standards for encryption (e.g., Virtual Private Networks) and strong pass-phrases. For any device Contractor utilizes to remotely connect to County's network, Contractor shall ensure the remote host device is not connected to any other network while connected to County's network, with the exception of personal networks that are under Contractor's complete control or under the complete control of a user or third party authorized in advance by County in writing. Contractor shall not use an open, unencrypted third party provided public WiFi network to remotely connect to County's network. Equipment used to connect to County's networks must: (a) utilize antivirus protection software; (b) utilize an updated operating system, firmware, and third party-application patches; and (c) be configured for least privileged access. Should Contractor exceed the scope of remote access necessary to provide the required services under this Agreement, as determined in County's sole discretion, County may suspend Contractor's access to County's network immediately without notice. Contractor must 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.

9. Article 14 of the Agreement is deleted and replaced in its entirety with the following (bold/underlining omitted):

ARTICLE 14
DATA AND NETWORK SECURITY

14.1 Data and Privacy. Contractor shall comply with all applicable data and privacy laws and regulations, including without limitation the Florida Information Protection Act of 2014, Florida Statutes Section 501.171, and shall ensure that County data processed, transmitted or stored in the System is not accessed, transmitted or stored outside the continental United States. Contractor may not sell, market, publicize, distribute, or otherwise make available to any third party any personal identification information (as defined by Florida Statutes Section 817.568 or Section 817.5685) that Contractor may receive or otherwise have access to in connection with this Agreement, unless expressly authorized in advance by County. If and to the extent 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.

14.2 Managed Services. Contractor shall immediately notify County of any terminations or separations of Contractor's employees who performed Services to County under the Agreement or who had access to County data**,** and Contractor must ensure such employees' access to County data and network is promptly disabled. Contractor must ensure all Contractor's employees with access to County's network via an Active Directory account comply with all applicable County policies and procedures when accessing

County's network. Contractor shall provide privacy and information security training to its employees with access the County's network upon hire and at least once annually. If any unauthorized party is successful in accessing any information technology component related to the Contractor, including but not limited to servers or fail-over servers where County data or files exist or are housed, Contractor shall report to County within twenty-four (24) hours of becoming aware of such breach. Contractor shall provide County with a detailed incident report within five (5) days after 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. Contractor shall not release County data or copies of County data without the advance written consent of County.

14.3 System and Organization Controls (SOC) Report. Prior to the commencement of any services, at least once annually, and upon request for the duration of the Agreement, Contractor must provide County with a copy of a current unqualified System and Organization Controls (SOC) 2 Type II Report for the Contractor, as well as any third party that provides hosting, SaaS, or data storage services for the Contractor platform, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy), unless the County's Chief Information Officer in his or her sole discretion approves other documentation of appropriate security controls implemented by Contractor. If the audit opinion in the SOC 2, Type II report is qualified in any way, Contractor shall provide sufficient documentation to demonstrate remediation of the issue(s) to the satisfaction of the County's Chief Information Officer.

14.4 Software Installed in County's Network. Contractor shall advise County of any third party software (e.g., Java, Adobe Reader/Flash, Silverlight) required to be installed and all versions supported. Contractor shall support updates for critical vulnerabilities discovered in applicable third party software. Contractor shall ensure that the Licensed Software is developed based on industry standards and best practices, including following secure programming techniques and incorporating security throughout the software-development life cycle. Contractor must develop and maintain the Licensed Software to operate on County-supported and approved operating systems and firmware versions. Contractor must mitigate critical or high risk vulnerabilities to the Licensed Software as defined by Common Vulnerability and Exposures (CVE) scoring system within 30 days of patch release. If Contractor is unable to apply a patch to remedy the vulnerability, Contractor must notify County of proposed mitigation steps to be taken and timeline for resolution. Contractor shall ensure the Licensed Software provides for role-based access controls and runs with least privilege access. Contractor shall support electronic delivery of digitally signed upgrades from Contractor's or the third-party licensor's website. Contractor shall enable auditing by default in software for any privileged access or changes. The Licensed Software must not be within three (3) years from Licensed Software's end of life date and the Licensed Software must run as least privilege without using fixed or default passwords. Contractor shall regularly provide County with end-of-

life-schedules for all applicable Licensed Software. Contractor will support encryption using at a minimum Advanced Encryption Standard 256-bit encryption keys ("AES-256") or current industry security standards, whichever is higher, for confidential data at rest. Contractor will use transport layer security (TLS) 1.1 or current industry standards, whichever is higher, for data in motion.

14.5 Payment Card Industry (PCI) Compliance. If and to the extent the Contractor Platform accepts, transmits or stores any credit cardholder data County or is reasonably determined by County to potentially impact the security of County's cardholder data environment ("CDE"), the following provisions shall apply: Contractor shall comply with the most recent version of the Security Standards Council's Payment Card Industry ("PCI") Data Security Standard ("DSS"). Prior to the Effective Date, after any significant change to the CDE, and annually Contractor shall provide to County: A copy of their Annual PCI DSS Attestation of Compliance ("AOC"); A written acknowledgement of responsibility for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the County, or to the extent that the service provider could impact the security of the county's cardholder data environment. A PCI DSS responsibility matrix that outlines the exact PCI DSS Controls are the responsibility of the service provider and which controls the service provider shares responsibility with the County. Contractor shall follow the VISA Cardholder Information Security Program ("CISP") payment Application Best Practices and Audit Procedures and maintain current validation. If Contractor subcontracts or in any way outsources the CDE processing, or provides an API which redirects or transmits County Data to a payment gateway, Contractor is responsible for maintaining PCI compliance for their API and providing the AOC for the subcontractor or payment gateway to the County. Mobile payment application providers must follow industry best practices such as VISA Cardholder Information Security Program ("CISP") or OWASP for secure coding and transmission of payment card data. Contractor agrees that it is responsible for the security of the County's cardholder data that it possesses, including the functions relating to storing, processing, and transmitting of the cardholder data. Contractor will immediately notify County if it learns that it is no longer PCI DSS compliant and will immediately provide County the steps being taken to remediate the noncompliant status. In no event should Contractor's notification to County be later than seven (7) calendar days after Contractor learns it is no longer PCI DSS complaint. Contractor shall enforce automatic disconnect of sessions for remote access technologies after a specific period of inactivity with regard to connectivity into County infrastructure. (PCI 12.3.8) Contractor shall activate remote access from vendors and business partners into County network only when needed by vendors and partners, with immediate deactivation after use. (PCI 12.3.9) Contractor shall implement encryption and two-factor authentication for securing remote access (non-console access) from outside the network into the County's environment with access to any stored credit card data. (PCI 8.3) Contractor shall maintain a file integrity monitoring program to ensure critical file system changes are monitored and approved with respect to County Data. (PCI 10.5.5) All inbound and outbound connections to County's CDE must use Transport Layer Security (TLS) 1.2 or current industry equivalent (whichever is higher).

10. The effective date of this Third Amendment shall be the date of complete execution by both Parties.

11. This Third Amendment may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

(The remainder of this page is blank.)

IN WITNESS WHEREOF, the parties hereto have made and executed this Agreement: BROWARD COUNTY through its BOARD OF COUNTY COMMISSIONERS, signing by and through its Mayor or Vice-Mayor, authorized to execute same by Board action on the _____ day of _____, 2019, and PIONEER TECHNOLOGY GROUP, LLC, signing by and through its _____, duly authorized to execute same.

BROWARD COUNTY

ATTEST:

_____
Broward County Administrator, as
ex officio Clerk of the Broward County
Board of County Commissioners

BROWARD COUNTY, by and through
its Board of County Commissioners

By_____
Mayor

____ day of _____, 2019

Approved as to form by
Andrew J. Meyers
Broward County Attorney
Governmental Center, Suite 423
115 South Andrews Avenue
Fort Lauderdale, Florida 33301
Telephone: (954) 357-7600
Telecopier: (954) 357-7641

By_____ 3/8/2019
René D. Harrod (Date)
Deputy County Attorney

NS/RDH
03/07/2019
Pioneer Technology Group Third Amendment
#413285.2

THIRD AMENDMENT TO SOFTWARE LICENSE AGREEMENT BETWEEN BROWARD COUNTY AND PIONEER TECHNOLOGY GROUP, LLC

PROVIDER

WITNESSES:

Signature

Sophia Gillett
Print Name of Witness

Signature

SARA C JOHNSON
Print Name of Witness

PIONEER TECHNOLOGY GROUP, LLC

By
Authorized Signor

Kevin Koon-Koon, Exe. Vice President, operations
Print Name and Title

8th day of March, 2019

ATTEST:

Patricia M. Dooley
Corporate Secretary or authorized agent

Notary Public State of Florida
Patricia M. Dooley
My Commission GG 223801
Expires 09/23/2022

(CORPORATE SEAL)