

Statement of Work For Printer Fleet Management Service



CONTENTS

| | | |
|-------|--------------------------------------------------|----|
| | Introduction | 1 |
| | Scope of Work | 1 |
| | Technical Questions | 2 |
| | Points of Contact | 4 |
| | Additional Requirements | 4 |
| | Period of Performance / Schedule | 5 |
| | Invoices and Payment / Acceptance Criteria | 5 |
| I. | Pricing | 5 |
| II. | Change Requests/Amendments | 6 |
| III. | Security Incident Notification | 6 |
| IV. | Vendor Response | 7 |
| V. | Signatures / Acceptance | 13 |
| VI. | Appendix A - MFD Requirements | 14 |
| VII. | | |
| VIII. | | |
| IX. | | |
| X. | | |
| XI. | | |

INTRODUCTION

The Employees Retirement System of Texas (ERS) is a trust fund established by the Texas Constitution and is described in Article XVI, Section 67, Texas Constitution. ERS is also organized pursuant to Subtitle B, Title 8, Texas Government Code, as well as Title 34 of the Texas Administrative Code, Sections 61.1, *et seq.* ERS invests and administers trust funds as a fiduciary for the exclusive benefit of the members and annuitants of the system. ERS also administers the Texas Employees Group Benefits Program,

- I. which consists of health benefits, life insurance and other optional benefits to participating individuals eligible to receive those benefits under applicable law.

SCOPE OF WORK

ERS requests a quote for printers and printer fleet management services. This quote includes but is not limited to the use of vendor-owned printers, auxiliary devices to improve security, software to track printing costs, and maintenance of the vendor printer fleet. The detailed description of the services is:

- II.
 - A. Install 27 multi-function devices (MFDs) which meet ERS feature requirements at ERS headquarters, located at 200 E. 18th St., Austin, Texas. MFDs include security badge readers, printers, scanners, and fax machines, which may be combined according to the normal specifications of the manufacturer. MFD feature requirements are found in Appendix A. Reports and statistics regarding ERS' print usage history is provided in the solicitation email.
While ERS will accept non-purchase leasing of the equipment, the preference is to rent MFD devices as part of the service.
 - B. Maintain MFD devices and ensure they perform their normal business function according to the original MFD feature requirements in this SOW. The services associated with this are:
 1. Monitor toner levels and deliver toner to the printer before toner cartridges are empty. Toner replacement can be performed by vendor staff or by ERS staff, depending on the team which is available when the toner cartridge is exhausted, Alternatively, vendor may supply an on-site reserve of toner for each model type of MFD, in quantities sufficient to prevent interruptions of service. ERS will not pay for toner until it is installed into a printer.
 2. Repair or replace malfunctioning MFDs to their original MFD feature requirements. The vendor must furnish all repairs, maintenance, toner, fusers, bulbs, and any other equipment, hardware and software for the Service at ERS headquarters. The vendor does not furnish paper.
 3. The service level between a report of a service issue and initial onsite response to ERS service of an MFD is four business hours. The service level between initial response and repair & return to ERS service of an MFD is within two business days. ERS business hours are from 7:30 AM – 5:30 PM Monday – Friday, except for Texas state designated holidays.
 - C. The vendor will help ERS secure printing, scanning, and faxing operations by providing and maintaining security badge readers for each MFD. Scanning and faxing operations cannot start without the use of an ERS badge. Authenticating an ERS badge will also deliver all pending jobs to the MFD. The vendor will provide the badge reader software, provide version, security and feature updates for the badge reader software, and train ERS staff in its use. Other security services provided to ERS are:
 1. Vendor must provide certificate of destruction and evidence of secure chain of custody for all hard drives or storage previously used at ERS. These must be provided to ERS within 60 days of storage removal from ERS. At the end of the contract, all storage must also be destroyed with a vendor-provided certificate of destruction and evidence of secure chain of custody. At ERS discretion, ERS may elect to destroy storage of specific MFD devices ourselves.
 2. All hard drives or storage in the MFD must be encrypted with at least 256 Bit symmetric key AES encryption. The vendor will provide annual verification of the encryption of the storage. [With WebJet Admin, ERS can verify at any time devices are in compliance. ImageNet will provide verification annually.](#)

- D. The vendor will provide and configure print management software for ERS to perform the following functions:
1. Provide ad hoc and scheduled reporting of print volume and user activity.
 2. Modify print rules as needed for printer outages or other appropriate situations.
 3. Route jobs automatically based on output color or number of pages to an alternate printer designated by administrator rule.
 4. Specify default output of the MFD as black/white for all print jobs or by classification of output for certain job types (e.g., all Outlook print jobs are black/white).
 5. Vendor will assist ERS in developing reports twice a year which show the cost of consumables by ERS (toner, paper) and the vendor will recommend actions to reduce printer fleet cost.
 6. Maintain print management software (HP Access Control Enterprise and HP Web Jetadmin and FMAudit) with the latest version, security, product updates and patches, and assist ERS staff during installation, testing, patching and upgrades of the software on the ERS network. The print management software is provided and maintained, updated, and patched by ImageNet included to ERS included in the monthly fee.

TECHNICAL QUESTIONS

- iii.
- A. What is the typical speed (print per minute) of a non-duplex color MS Word document?
- a) 50 pages per min on the larger machines
 - b) 45 pages per min on the desktop machines
- B. What is the typical speed (print per minute) of a non-duplex black and white MS Word document?
- a) 50 pages per min on the larger machines
 - b) 45 pages per min on the desktop machines
- C. How long is the time between the badge/security validation at the printer and the ejection of the first printed page? a) 8 seconds color
- D. How often does the Respondent conduct basic/preventative maintenance on each MFD to avoid breakdowns? Describe this maintenance.
- a) ImageNet Consulting's service practice is to have a "TOTAL CALL" performed on each service visit. This covers the fix to the problem initially reported, but also a complete inspection of the device while on site. The technician will inspect the PM Call guidelines by the manufacturer and check service history for the last meter on the last PM/Service Call. This helps to maximize the impressions between service calls, so the end users can be more productive doing what they are paid to do without printer issues.
- E. What training will the Respondent provide to ERS print administrators and how long are the training sessions?
- a) Training is unlimited throughout the life of the contract. Our training process starts once the device is delivered where we conduct basic user training. We then follow up with a scheduled training session with key operators and other admin staff that wish to know more about tools to maximize the use of the machine and improve business processes. We also have customized quick reference cards and we can collaborate with ERS to create custom videos for additional support.
- F. Describe the process for requesting MFD service.
- a) There are 3 methods to placing a service call
 - Call 1.800.937.2647 and speak to a live person. Just have the equipment ID ready so we know which device is in question.
 - Email service@imagenet.com with the equipment ID, state the issue, and hit send. A response will be sent back within the hour along with an ETA for when the tech will arrive
 - Log on to imagenet.com/myaccount to place the service call. ERS will be given custom accounts so users can place calls online if they desire.

- G. How long will the Respondent require to install the devices at ERS?
- a) 2 days is the estimated time for implementation of all 27 units. The best practice is to work with IT to setup the 3 software packages- FM AUDIT, HP WebJet Admin, and HP Access Control Enterprise. Once the software is setup we will deliver a test unit, configure, and set as the unit to be cloned with HP WebJet Admin. This will help the turnaround time once the hardware is delivered.
- H. Describe the security reporting from the MFD.
- a) Each of the HP devices come standard with
 - HP SureStart- during the startup the integrity of the boot code or BIOS is validated with the GOLDEN IMAGE
 - Whitelisting- when loading firmware only authentic, digitally signed by HP firmware can be loaded
 - Run Time intrusion detection- during run time, HP printers detect and prevent unexpected changes to memory.
 - HP Connection Inspector- When connecting to the network, HP Enterprise Printers put a stop to suspicious requests
 - Secure Encrypted Print for GDPR Compliance through the use of the HP Universal Print Driver
 - b) Optional HP JetAdvantage Security Manager allows you to proactively monitor and deploy security policies to the printer fleet
- I. Describe the procedure for secure destruction of hard drives or storage when MFD devices are returned for service or at the end of the contract.
- a) ImageNet will work with ERS to ensure the device HDD's are met with the highest encryption and wipe standards before any machines leave the property
- J. Describe any other features of the MFD not previously mentioned.
- a) ESKER Fax Server integration to eliminate the need for ANALOG lines. Out of the box the HP devices integrate seamlessly with ESKER LANFAX and PULSE
 - b) Mobile printing
 - c) Office 365 integration with SharePoint, OneDrive, and Laserfiche
 - d) Predictive problem resolution through FM AUDIT/Jet Advantage MNGR
- K. Describe the proposed installation and setup of MFDs, software installations, and ERS training.
- a) Day 1 contract execution
 - b) Day 1 hardware orders
 - c) Week 2 FM AUDIT, HP WebJet Admin and Access Control Enterprise installed (software)
 - d) Week 2 Test Units (HP e87660z and e57540c) delivered and configured with IT group
 - e) Week 2 Hardware received at warehouse and assembled
 - f) Week 3 fleet implementation
 - g) Week 3 basic training and key operator training conducted
 - h) Ongoing- Throughout the process our ImageNet Project Manager will work with the ERS key point of contact for communications and project updates
- L. Please attach answers to these questions along with your proposal to this SOW, along with a method to view a video demonstration of the MFD devices.

Access Control Enterprise: <http://hp.brightcovegallery.com/products/detail/video/4270907774001/hp-access-control-printing-solutions?autoStart=true&q=HP%20Access%20Control>

HP e87660z overview: <https://www.youtube.com/watch?v=AUD714tsAcc>

HP e87660z replace toner: <https://www.youtube.com/watch?v=OYOIKuX57eI>

HP Security: <https://youtu.be/OELyD9HiFgI>

ImageNet Overview: <https://www.youtube.com/watch?v=G-BYCVyOvhA>

Live video session available upon request.

POINTS OF CONTACT

The contact for this SOW solicitation will be the IS Administration section; they can be contacted at isadministration@ers.texas.gov.

IV. After award, contract communications for this SOW must be directed to ERS Contract Manager:
Joanna Gonzalez
200 E. 18th Street, Austin, Texas 78701
(512) 867-7137
joanna.gonzalez@ers.texas.gov

After award, project issues must be coordinated with the ERS Project Manager:
Sylvia Montemayor
200 E. 18th Street, Austin, Texas 78701
(512) 867-7120
sylvia.montemayor@ers.texas.gov

After award, security issues must be coordinated with the ERS Chief Information Security Officer:
Matt Remiersma
200 E. 18th Street, Austin, Texas 78701
(512) 867-7308
matt.remiersma@ers.texas.gov

V. **ADDITIONAL REQUIREMENTS**

Any changes to the SOW scope of work requirements must be reflected in the response to this document.

- A. ERS will review and approve vendor's standard Certificate of Insurance (COI) prior to commencement of services.
- B. The vendor agrees to sign a Business Associate Agreement and Data Breach and Security Notification Agreement for the term of this engagement.
- C. Texas Government Code, Section 2054.5192 requires any Vendor, or a subcontractor, officer, or employee of Vendor, who will have access to a state computer system or database, to receive cyber security training. The Vendor shall ensure that all such employees and subcontractors have completed the required cybersecurity training. ERS will accept proof of security awareness training from programs certified by the Texas Department of Information Resources. ERS also provides cybersecurity training for all Vendor staff and subcontractors receiving logins to ERS systems. (<https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Certified%20Training%20Programs.docx>)
- D. For transactions under this agreement, the order of precedence is the DIR master contract and appropriate DIR appendixes, and Statement of Work For Printer Fleet Management Service (this document).
- E. If the selected DIR Prime Vendor decides to subcontract any part of the SOW or contract in a manner that is not consistent with DIR's HUB subcontracting plan (Appendix B of the DIR Cooperative Contract), the selected DIR Prime Vendor must comply and submit a revised HUB subcontracting plan to DIR before subcontracting any of the work under the SOW. No work may be performed by a subcontractor before DIR has approved a revised HSP for the Cooperative Contract.

PERIOD OF PERFORMANCE / SCHEDULE

The term of project service for this Statement of Work is for three (3) years and commences upon signature by all parties on the Signature page. The term may be extended for two (2) additional, one (1) year extensions. The total project service is not planned to exceed five (5) years, including all initial and service extensions. ERS will only pay monthly fees for equipment which is installed at the ERS headquarters.

VI. **INVOICES AND PAYMENT / ACCEPTANCE CRITERIA**

The vendor agrees that ERS will review all service and devices associated with this SOW. The vendor agrees that ERS is the sole determination of completeness of the services, and final acceptance all services by the vendor is dependent upon acceptance by ERS.

- VII. The vendor must submit invoices to ERS by mail: P.O. Box 13207, Austin, Texas 78711-3207, or by email: ap@ers.texas.gov with cc: isadministration@ers.texas.gov.

PRICING

The pricing listed below includes all the SOW costs – these are the fixed-fee costs to deliver the services described in the SOW. ERS is a tax-exempt Texas state agency; billing for taxes is not allowed.

VIII.

HP Color LaserJet Fleet

| Description | 36 Month Cost | 48 Month Cost | 60 Month Cost |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Phase 1 – Setup (all installation and configuration tasks) | \$0 | \$0 | \$0 |
| Phase 2 – Ongoing monthly charge | \$4,510.24 | \$3,302.07 | \$3,124.13 |
| Additional costs not specified above (please list them) | \$.0099 per mono page / \$.049 per color page OPTIONAL: Security Manager for 27 licenses and installation/support is \$186/month. Each additional unit is \$6.88/month @ 36 months | \$.0099 per mono page / \$.049 per color page OPTIONAL: Security Manager for 27 licenses and installation/support is \$202.91/month. Each additional unit is \$7.52/month @ 60 months | \$.0099 per mono page / \$.049 per color page OPTIONAL: Security Manager for 27 licenses and installation/support is \$202.91/month. Each additional unit is \$7.52/month @ 60 months |
| Cost for an additional MFD (additional monthly charge) HP E87650Z | \$192.23 | \$145.91 | \$133.15 |
| Cost for an additional MFD (additional monthly charge) HP E87640Z | \$173.00 | \$131.31 | \$119.83 |
| Cost for an additional MFD (additional monthly charge) HP E57540C | \$75.39 | \$59.31 | \$52.22 |

SERVICE RELIABILITY

HP technology affords additional benefits in user productivity with a very low service intervention rate. The device does not have traditional service requirements to replace items like Fusers, Transfer Belts, and imaging components. This leads to very long intervals between required service events increasing user productivity. Additionally, supplies intervention is extremely easy with only 4 long life supplies (Black, Cyan, Magenta, Yellow) that last up to 50,000 pages before needing replacing. There are no other consumables and dramatically less interventions and packaging waste than competing devices.

Additionally, because the device does not have a fuser the devices require up to 80% less power than competing devices.

The vendor must have staff available to answer questions regarding billing and invoices.

CHANGE REQUESTS/AMENDMENTS

- IX. ERS and vendor affirm they are fully committed to successful delivery of services. Both ERS and vendor must review any scope changes and SOW Amendments. Moreover, DIR must approve, in writing, material changes to the SOW requiring an increase in price prior to implementation of changes. The following procedure governs the change request/Amendment process:
- A. ERS and the vendor's staff will discuss the proposed change request and mutually agree on the scope of the change.
 - B. ERS and the vendor's representative will document the proposed change for review by parties authorized to sign change requests or Amendments. This may include:
 - 1. The impact to the project schedule and cost impact, if any.
 - 2. Modifications to the original SOW agreement listing sections of the original SOW that are being amended/changed (*i.e.* where changes to requirements in original SOW are being modified, adding section for enhancements)
 - 3. Changes to Order of Precedence
 - 4. Changes to vendor DIR number, if necessary
 - 5. Extensions to the contract timeline and project milestones
 - 6. Purpose of the change
 - 7. Parties involved in the successful delivery of the change (subcontractors, vendor or ERS staff, etc.)
 - 8. Pricing changes from the original SOW and modifications necessary for additional services (if applicable)
 - 9. The change request and amendments form must include ERS and vendor signature blocks (to include name, company, title, date, and signature), as well as a signature block for the Texas Department of Information Resources (if required).
 - C. The vendor and ERS will sign the change request, which contains the information listed in steps above. If required, the partially executed document will also be sent to DIR to review, approve and sign.
 - X. D. ERS will execute the Purchase Order Change Notice (POCN) to the purchase order or create a new purchase order.
 - E. The duly authorized ERS representative who may approve change orders and pricing increases is the ERS Executive Director or his designee.

SECURITY INCIDENT NOTIFICATION

The vendor shall reply to security incidents in the manner described in the DIR contract. If there are no descriptions of security incident notification in the DIR contract, the vendor must notify ERS when a data breach occurs which may affect ERS data as detailed in the Data Breach and Security Notification Agreement.

VENDOR RESPONSE

Use this section to provide descriptions of the changes and clarifications to the SOW services, as well as any vendor-specific detail, vendor service capability and vendor staff capability to deliver the services specified in the SOW.

XI.

Client Responsibilities

| | |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| • | Client to identify and provide an IT Administrator for solution implementation and support interaction. |
| • | Client will provide access to all areas required to complete this project. Any areas of high security or hazard should be made known prior to project commencement. |
| • | Client will provide access to all information and documentation required to complete this project. |
| • | Client will provide an onsite contact person responsible for providing direction and approvals on completion of work. |
| • | Client will directly provide all non-ImageNet provided hardware and software support required unless specifically indicated otherwise. Client will provide Minimum Server Requirements defined in Vendor Questionnaire documents in order to successfully install and maintain the solutions referenced in the SOW. |
| • | Client will ensure that any Client provided virtual servers will meet all required specifications for software. |
| • | Client will assure that all required LAN/WAN access and administrative rights are made available to complete the installation. |
| • | Client is solely responsible for back-up of system and database. Client is solely responsible for back-up of system and database according to common procedures and where explained in solution documentation. For HP Web Jetadmin, see http://h10032.www1.hp.com/ctg/Manual/c01943154 |
| • | Client and Vendor will work together to develop a mutually agreeable timeline. We will need access to the servers with minimum requirements either through a remote connection or joint session in order to install/configure the software solutions provided. |
| • | Client will secure SSL Certificate for chosen Server host names when applicable. Internally generated Certificates will be produced by client as vendor is not responsible for this task. |
| • | Client is responsible to setup initial environment that meets Platform Requirements listed in the vendor questionnaire document. Should any other applications be running on this server, it is the responsibility of the client to notify our engineers before they begin to access the system. |
| • | All System Engineer work outside of the work outlined in Section II.D.6. of the SOW is billed at \$225.00 per hour. |

Assumptions & Terms

The ongoing monthly charge is based on a commitment that work is to be performed during regular business hours; 7:30AM to 5:30PM local time, Monday through Friday, except for Texas state designated holidays.

Disclaimers

- ImageNet Consulting is not responsible for the loss of data due to system failure and lack of database back-up

Add Minimum Server Requirements Appendix

| System Requirements HP ACCESS CONTROL ENTERPRISE | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Is your Product hosted on a customer's infrastructure or your facilities? | Customer Infrastructure |
| Installation hardware requirements – (CPU, memory, storage) | 4 vCPUs, 12GB RAM, 80GB HDD |
| Installation software stack (OS, web-server, app-server, DBMS, middleware, .NET runtime virtual machine, JAVA runtime virtual machine, etc.) [NOTE: ERS enterprise standards are Windows Server 2012 R2, and secondarily, SUSE Linux Enterprise Server 12. ERS will also support VMware virtual appliances.] | <p>Windows Server 2016 or 2019 .NET Framework 3.5 .NET Framework 4.7.2 or 4.8 Internet Information Services (IIS) Crystal Reports for .NET Framework 2.0 (x64) Microsoft Access Database Engine 2010 Visual C++ 2008 Redistributable (x64) Visual C++ 2015-2019 Redistributable (x64) Visual C++ 2015-2019 Redistributable (x86) SQL Server 2008 R2 Analysis Services OLE DB Provider Microsoft SQL 2008 R2 Native Client Microsoft SQL 2012 Native Client Microsoft SQL Server Compact 4.0 SP1 (x64) HP Access Control Enterprise 16.8 Optional – Adobe Acrobat Reader Optional – Microsoft Office</p> <p>NOTES -Solution requires an SQL Database [HPACJA] - 30 GB -Solution requires an SQL Database [HPACIRM] - 1 GB -Domain Service Account with local Administrators group membership on server -Service Account also is dbo for databases Print management software database can be on the latest Microsoft SQL Server 2019 and on a SQL Farm.</p> |
| Are there known security patches required before installation (such as with Windows server, IIS or other middleware)? | None. Latest patches recommended, not required. |
| Does your staff require Administrative permissions and remote user access for installation & configuration on our platform? | Admin rights required for installation and for service to operate post-installation |
| Does this software require Active Directory (Windows) or Linux security management? | Yes |
| What environments are needed or recommended (e.g. development, test, production, verification, patch) | Flexible to customer's policy |

| System Requirements HP WEBJET ADMIN | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Is your Product hosted on a customer's infrastructure or your facilities? | Customer Infrastructure |
| Installation hardware requirements – (CPU, memory, storage) | 4 vCPUs, 12GB RAM, 80GB HDD (assuming DB on separate server) |
| Installation software stack (OS, web-server, app-server, DBMS, middleware, .NET runtime virtual machine, JAVA runtime virtual machine, etc.) [NOTE: ERS enterprise standards are Windows Server 2012 R2, and secondarily, SUSE Linux Enterprise Server 12. ERS will also support VMware virtual appliances.] | Windows Server 2016 or 2019 .NET Framework 3.5 .NET Framework 4.7.2 or 4.8 Visual C++ 2015-2019 Redistributable (x64) Visual C++ 2015-2019 Redistributable (x86) HP Web Jetadmin 10.4 SR7 NOTES -Solution requires an SQL Database [HPWJA] - 30 GB -Domain Service Account with local Administrators group membership on server -Service Account also is dbo for database Print management software database can be on the latest Microsoft SQL Server 2019 and on a SQL Farm. |
| Are there known security patches required before installation (such as with Windows server, IIS or other middleware)? | None. Latest patches recommended, not required. |
| Does your staff require Administrative permissions and remote user access for installation & configuration on our platform? | Admin rights required for installation and for service to operate post-installation |
| Does this software require Active Directory (Windows) or Linux security management? | Yes |
| What environments are needed or recommended (e.g. development, test, production, verification, patch) | Flexible to customer's policy |

| System Requirements HP SECURITY MANAGER | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Is your Product hosted on a customer's infrastructure or your facilities? | Customer Infrastructure |
| Installation hardware requirements – (CPU, memory, storage) | 2 vCPUs, 8GB RAM, 60GB HDD |
| Installation software stack (OS, web-server, app-server, DBMS, middleware, .NET runtime virtual machine, JAVA runtime virtual machine, etc.) [NOTE: ERS enterprise standards are Windows Server 2012 R2, and secondarily, SUSE Linux Enterprise Server 12. ERS will also support VMware virtual appliances.] | Windows Server 2016 or 2019 .NET Framework 3.5 .NET Framework 4.7.2 or 4.8 Internet Information Services (IIS) Visual C++ 2015-2019 Redistributable (x64) Visual C++ 2015-2019 Redistributable (x86) Windows SDK Signing Tools HP Print License Service (includes Flexera) HP JetAdvantage Security Manager 3.4 NOTES -Solution requires an SQL Database [HPIPSC] - 10 GB -Domain Service Account with local Administrators group membership on server -Service Account also is dbo for database Print management software database can be on the latest Microsoft SQL Server 2019 and on a SQL Farm. |
| Are there known security patches required before installation (such as with Windows server, IIS or other middleware)? | None. Latest patches recommended, not required. |
| Does your staff require Administrative permissions and remote user access for installation & configuration on our platform? | Admin rights required for installation and for service to operate post-installation |
| Does this software require Active Directory (Windows) or Linux security management? | Yes |
| What environments are needed or recommended (e.g. development, test, production, verification, patch) | Flexible to customer's policy |

Add Hardware and Software List Appendix- DIR- TSO - 4159



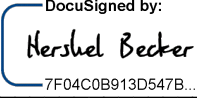
| HP LASER Devices | | |
|-------------------------|--------------------------------------------|------------|
| SKU | Device | Qty |
| X3A76A | HP Color LaserJet Dept Mgd Flw MFP Prntr | 8 |
| X3A89A | HP Color LaserJet MFPE87650z Speed License | 8 |
| Y1F98A | HP LaserJet Dual Cassette Dprtmnt Feeder | 8 |
| Y1G00A | HP LaserJet Inner Finisher | 8 |
| 2EH31A | HP MFP Analog 700 Fax Accessory | 8 |
| G8Y25AAE | HPAC (need to include install PS) | 8 |
| X3D03A | Card Reader | 8 |
| UA0E2E | HP 3y 9x5 HPAC Enter Supp | 8 |
| U9RR4E | HP JA install/config | 8 |
| SKU | Device | Qty |
| X3A86A | HP Color LaserJet 87640z Dept MFP Prntr | 14 |
| Y1F98A | HP LaserJet Dual Cassette Dprtmnt Feeder | 14 |
| Y1G00A | HP LaserJet Inner Finisher | 14 |
| 2EH31A | HP MFP Analog 700 Fax Accessory | 14 |
| G8Y25AAE | HPAC (need to include install PS) | 14 |
| X3D03A | Card Reader | 14 |
| UA0E2E | HP 3y 9x5 HPAC Enter Supp | 14 |
| U9RR4E | HP JA install/config | 14 |
| SKU | Device | Qty |
| 3GY26A | HP Color LaserJet MgdFlwMFPE57540c Prntr | 5 |
| G8Y25AAE | HPAC (need to include install PS) | 5 |
| X3D03A | Card Reader | 5 |
| UA0E2E | HP 3y 9x5 HPAC Enter Supp | 5 |
| U9RR4E | HP JA install/config | 5 |
| | | |

FM AUDIT for all units

HP WebJet Admin for all Units

HP Access Control Enterprise and Card Readers for all Units

XII. SIGNATURES / ACCEPTANCE

| | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Accepted by: Ryan Starks ImageNet Consulting Signature: </p> <hr/> <p>Print Name: Ryan Starks Title: Vice President, Austin Date: 2.1.2021 DIR Contract #: __DIR-TSO-4159</p> | <p>Accepted by: Employees Retirement System of Texas Signature: </p> <hr/> <p>Print Name: Porter Wilson Title: Executive Director Date: <u>2.11.2021</u></p> |
| | <p>Accepted by: Texas Department of Information Resources Signature:  <small>7F04C0B913D547B...</small></p> <hr/> <p>Print Name: Hershel Becker Title: Chief Procurement Officer Date: <u>2/23/2021 6:21 PM CST</u></p> |

- Attachment A – MFD Requirements
- Attachment B – Business Associate Agreement
- Attachment C – Data Security and Breach Notification Agreement

APPENDIX A - MFD REQUIREMENTS

22 – Large-factor MFD devices with scanners, fax, printers, security devices

5 – Desktop MFD devices with like-equipment above, for single-user counseling offices

MFD Services and Features

1. Each MFD is self-contained on one vertical steel cart with casters, with one cord to a 20 amp circuit with t-slot 20A/250V 3wire 2 pole receptacle with a NEMA 6-20 rating.
2. The printer administrator is designated by an Active Directory group, with authentication of the group members by ERS Active Directory

MFD Faxing Requirements

3. Each MFD must be able to send faxes and the faxing function must support faxing via the T.38 protocol.
4. The MFDs shall only be used for outbound faxing; ERS uses a different service for inbound faxing.

MFD Network Requirements

5. Each MFD must connect to the ERS network via a wired 1Gbps RJ45 ethernet connection
6. ERS shall maintain and be responsible for the internal network and telephony system that supports Voice-over-IP and T.38; Respondent will be responsible for configuring the network and faxing settings on the MFDs at the direction of ERS.
7. WiFi (802.11) and Bluetooth communication options for sending print jobs to the MFD are not requested, and such features must be removed or disabled if the equipment proposed supports these communication technologies.

MFD Printing Requirements

8. Each MFD must have the ability to collate.
9. Each MFD must have the ability to print on plain letter, plain legal, plain tabloid and bonded letter.
10. Each MFD must have the ability to print single-sided or duplex documents.
11. Each MFD must have the ability to staple collated copies.
12. Each MFD must support black and white and greyscale printing.
13. Each MFD must support color printing.
14. **{OPTIONAL FEATURE}** - User could have the ability to re-print completed print jobs for a pre-determined set of time (7days).

MFD Scanning Requirements

15. Each MFD must have at least a 25 document-feed into scanner.
16. Each MFD must have the ability to scan a document and email the scanned PDF to an email recipient.
17. Each MFD must have the ability to scan and check-in documents to a Sharepoint 2016 library .
18. Each MFD must have the ability to scan Letter, Legal and 11"x14" sized paper.
19. Each MFD scanner must have the ability to deliver a PDF document, after performing OCR scan to text translation.
20. Each MFD scanner must have the ability to scan single-sided and duplex documents.
21. MFD scanners must scan in full color, with a minimum of 300 DPI.

Security Requirements

22. The driver for the print release queue must be Microsoft certified.
23. Drivers for the MFD printers must maintain Microsoft certification support within three months of new, general release of operating systems, feature packs, or service packs.
24. All print jobs must wait in a single print queue for end-user authentication at the badge reader on the MFD prior to printing.
25. The MFD proposed must not transmit print or scan job information outside of ERS' network, except when used as a fax machine by an authorized ERS badged user..

**BUSINESS ASSOCIATE AGREEMENT
BETWEEN EMPLOYEES RETIREMENT SYSTEM OF TEXAS
AND ImageNet Consulting, LLC**

This Business Associate Agreement (“Agreement”) is effective upon execution by and between the Employees Retirement System of Texas (hereinafter “Health Plan” or “Covered Entity”) and ImageNet Consulting, LLC (hereinafter “Business Associate”). Health Plan and Business Associate may be individually referred to as a “Party” and collectively as the “Parties.”

PREAMBLE

WHEREAS, the requirements of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH”), as incorporated in the American Recovery and Reinvestment Act of 2009, and the implementing regulations issued and amended by the U.S. Department of Health and Human Services Secretary (“Secretary”) (45 CFR Parts 160 and 164, known as the “Privacy and Security Rules,” require the Parties to reach agreements regarding the privacy, security and breach notification requirements related to ‘*protected health information*,’ as clarified by the Genetic Information Nondiscrimination Act of 2008 (“GINA”), Public Law 110-233 and applicable regulations (PHI) (these requirements are hereinafter collectively referred to as “HIPAA”)); and

WHEREAS, Health Plan is a ‘*Covered entity*’ under HIPAA in that it is a covered group health plan, and as a covered entity must ensure the privacy and security of all PHI which its Business Associate ‘*uses*’ or ‘*discloses*,’ and

WHEREAS, Health Plan and Business Associate have entered into a Statement of Work governed by DIR Contract No. 4159 (the “Contract”) under which Business Associate contracted to provide certain functions, activities, or services (collectively “Services”) to Health Plan, and in the continued performance of these Services may create, receive, use, disclose, or have access to PHI from or on behalf of Health Plan; and

WHEREAS, in performing Services for Health Plan, Business Associate is considered a ‘*Business Associate*’ as this term is defined in HIPAA; and

WHEREAS, the Parties agree that this Business Associate Agreement shall be attached to the Statement of Work as Attachment “B to incorporate therein for all purposes as if restated in full the terms of this Agreement; and

WHEREAS, HIPAA mandates that a ‘*Covered Entity*’ enter into agreements with their ‘*Business Associates*’ to ensure the continued privacy and security of PHI; and

WHEREAS, the Parties desire to comply with HIPAA; and

WHEREAS, this Agreement is intended to ensure that Business Associate will establish and implement appropriate safeguards (including certain administrative and security requirements) for the PHI the Business Associate may create, receive, use, disclose, or have access to in connection with Services by Business Associate to Health Plan.

NOW THEREFORE, in consideration of the Parties' continuing obligations under the Contract, in compliance with HIPAA, and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, the Parties agree to the provisions of this Agreement in order to address the statutory obligations imposed upon them and to protect the interests of the Parties.

SECTION I. DEFINITIONS

The following capitalized terms are defined in 45 CFR Parts 160 and 164. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms are defined in 45 CFR Parts 160 and 164. References herein to the Privacy and Security Rules, or a specific section thereof, shall mean the section as in effect or as amended.

- 1.1 *'Breach'* means the acquisition, access, use, or disclosure of PHI in a manner not permitted under 45 CFR §§ 164.500 et seq. (Subpart E) of this part which compromises the security or privacy of the protected health information. As set forth in 45 CFR 164.401(2), except as provided in 45 CFR 164.401(1), an acquisition, access, use or disclosure of protected health information in a manner not permitted under Subpart E is presumed to be a breach unless Health Plan or Business Associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated. Further, a use or disclosure of protected health information that does not include the identifiers listed at 45 CFR § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information. *'Breach'* excludes unintentional, inadvertent and/or unretainable breaches, as defined by 45 CFR 164.402(1).
- 1.2 *'Electronic Protected Health Information'* means PHI that is created, received, stored, maintained, processed and/or transmitted in an electronic format.
- 1.3 *'Health Information'* means any information, including *'genetic information,'* whether oral or recorded in any form or medium, that: (1) is created or received by a *'Health Care Provider,' 'Health Plan,'* public health authority, employer, life insurer, school or university, or *'Health Care Clearinghouse;'* and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
- 1.4 *'Individually Identifiable Health Information'* means information that is a subset of *'Health Information,'* including demographic information collected from an individual, and: (1) is created or received by a *'Health Care Provider,' 'Health Plan,'* employer, or *'Health Care Clearinghouse;'* and (2) relates to the past, present, or future physical or mental health or

condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

- 1.5 ‘*Protected Health Information*’ (“PHI”) means Individually Identifiable Health Information: (1) except as provided in section (2) of this definition, that is (a) transmitted by electronic media; (b) maintained in any medium described in the definition of ‘electronic media’ found at 45 CFR § 160.103; or (c) transmitted or maintained in any other form or medium. (2) Protected Health Information excludes Individually Identifiable Health Information in (i) education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g; (ii) records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); (iii) employment records held by a Covered Entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years.
- 1.6 ‘*Subcontractor*’ means a person to whom a ‘*Business Associate*’ delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
- 1.7 ‘*Workforce*’ means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Business Associate, is under the direct control of Business Associate, whether or not they are paid by Business Associate.
- 1.8 ‘*Unsecured PHI*’ means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 on the U.S. Department of Health and Human Services (“HHS”) website.
- 1.9 For purpose of security requirements, 45 CFR Part 164 Subpart C: ‘*Availability*’ means the property that data or information is accessible and useable upon demand by an authorized person. ‘*Confidentiality*’ means the property that data or information is not made available or disclosed to unauthorized persons or processes. ‘*Integrity*’ means the property that data or information have not been altered or destroyed in an unauthorized manner.

SECTION II. GENERAL TERMS

- 2.1 This Agreement shall remain in effect for a period coterminous with the Contract and any extensions, amendments and renewals thereof.
- 2.2 Except as otherwise might be defined herein, all terms first appearing in ‘single’ quotation marks and italicized shall have the same meaning set forth in HIPAA, including 45 CFR §§ 164.103, 164.105, 164.304, 164.501 and 164.502.
- 2.3 In the event of an inconsistency between the terms of this Agreement and the mandatory terms of HIPAA, the mandatory terms of HIPAA shall prevail. Where the terms of this Agreement are different from those included in HIPAA but the terms of HIPAA are permissive, the terms of this Agreement shall control.

- 2.4 The terms of HIPAA may be expressly amended from time to time by Legislation, HHS, or as a result of interpretations by HHS, a court, or another regulatory agency with authority over the Parties. In such an event, the Parties will work together in good faith to determine the impact on the Parties' obligations and whether the specific event requires the need to amend this Business Associate Agreement. In any situation under the Business Associate Agreement where a question arises as to the applicability of state or federal law or regulations to the Health Plan, then Health Plan's interpretation of the applicability of such law or rule shall control.
- 2.5 The Parties agree to take such action as necessary to amend this Agreement from time to time as is necessary to comply with HIPAA, the Privacy and Security Rules and HITECH.
- 2.6 Any ambiguity in this Agreement shall be resolved to permit compliance with HIPAA and HITECH.
- 2.7 Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.
- 2.8 This Agreement does not create or confer any rights or remedies onto third parties.
- 2.9 Modification of the terms of this Agreement shall not be effective or binding upon the Parties unless and until such modification is committed to writing and executed by the Parties hereto.
- 2.10 This Agreement shall be binding upon the Parties hereto, and their respective legal representatives, trustees, receivers, successors and permitted assigns.
- 2.11 Should any provision of this Agreement be found unenforceable, it shall be deemed severable and the balance of the Agreement shall continue in full force and effect as if the unenforceable provision had never been made a part hereof.
- 2.12 To the extent not preempted by federal law, this Agreement and the rights and obligations of the Parties hereunder shall in all respects be governed by, and construed in accordance with, the laws of the state of Texas, including all matters of construction, validity and performance.
- 2.13 All notices and communications required or permitted to be given hereunder shall be delivered by certified mail, first class postage prepaid or via first class mail, with a copy by email, to the individual(s) listed in Section VII. Notices, or at such other address as such Party shall from time to time designate in writing to the other Party, and shall be effective from the date of mailing. Either party may waive the requirement for a particular notice or communication to be delivered via certified mail or first class mail and instead accept it solely by email. Further, either party may change its notice information by sending written notice of such change to the other party in the manner set forth above, without any requirement to amend this Agreement.
- 2.14 This Business Associate Agreement, including such portions as are incorporated by reference herein, constitutes the entire Business Associate Agreement by, between and among the Parties, and such Parties acknowledge by their signature hereto that they do not rely upon any representations or undertakings by any person or Party, past or future, not expressly set forth in writing herein. In the event of a conflict between the Contract and

this Business Associate Agreement, the conflict shall be resolved to permit compliance with HIPAA and HITECH.

- 2.15 These provisions shall survive termination of this Agreement: 4.7, 4.8, 4.9, 4.10, 4.14, 4.15, 4.16 and 4.18.

SECTION III. SPECIFIC PERMITTED AND REQUIRED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

3.1 Business Associate agrees to create, receive, *'use,'* or *'disclose'* PHI only in a manner that is consistent with this Agreement and HIPAA, or as permitted or required by law, and in connection with providing the Services to Health Plan identified in the Contract. Accordingly, in providing Services to or for Health Plan, Business Associate, for example, will be permitted under HIPAA to:

- (1) *'use'* and *'disclose'* PHI for *'treatment,'* *'payment,'* or *'health care operations.'*
- (2) de-identify PHI and maintain such de-identified health information indefinitely; provided that all identifiers are destroyed or returned in accordance with this Agreement.
- (3) create a *'limited data set,'* provided that Business Associate:
 - (a) does not *'use'* or further *'disclose'* PHI contained in the *'limited data set'* except as necessary to provide the Services or as provided for in this Agreement or otherwise *'required by law;'*
 - (b) uses appropriate Safeguards to prevent the *'use'* or *'disclosure'* of PHI contained in the *'limited data set'* other than as provided for by this Agreement;
 - (c) reports to Health Plan any *'use'* or *'disclosure'* of PHI contained in the *'limited data set'* of which Business Associate becomes aware that is not provided for by this Agreement;
 - (d) ensures that any agents or subcontractors to whom it provides access to the *'limited data set'* agree to the same restrictions and conditions that apply to Business Associate under this Agreement; and
 - (e) does not re-identify PHI or contact the *'individuals'* whose information is contained within the *'limited data set.'*

3.2 Additionally, under HIPAA, Business Associate may *'use'* or *'disclose'* PHI received by the Business Associate in its capacity as a Business Associate to Health Plan to perform functions, activities, or services for, or on behalf of, Health Plan as specified in the Contract.

Further, Business Associate may *'use'* or *'disclose'* PHI if:

- (1) The use relates to: (a) the proper management and administration of the Business Associate or to carry out legal responsibilities of the Business Associate, or (b) data aggregation services relating to the health care operations of Health Plan.

For purposes of this Agreement, the following terms shall have the meanings identified:

- (i) *'data aggregation services'* shall mean the combining of PHI by Business Associate with the PHI received by Business Associate in its capacity as a Business Associate of another covered entity, to permit data analyses that relate to the health care operations of Health Plan or another covered entity, and
- (ii) *'legal responsibilities'* of the Business Associate shall mean responsibilities imposed by law or regulation but (unless otherwise expressly permitted by Health Plan) shall not mean obligations Business Associate may have assumed pursuant to contracts, agreements, or understandings with entities other than Health Plan.
- (2) The disclosure of information received in such capacity is for the proper management and administration of the Business Associate or to carry out its legal responsibilities and, when the law requires such disclosure, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidential and the person agrees to notify the Business Associate of any breaches of confidentiality. In this regard, *'required by law'* shall have the meaning set forth in HIPAA.

- 3.3 Business Associate may use and disclose PHI to report violations of law to appropriate federal and state authorities, consistent with 45 CFR 164.502 (j)(i).

SECTION IV. OBLIGATIONS OF BUSINESS ASSOCIATE

- 4.1 To the extent such agreements are otherwise permitted under the Contract, Business Associate shall include in all agreements or contracts with its agents, contractors, subcontractors or vendors, if such agreements or contracts involve Business Associate's *'disclosure'* to or *'use'* by the agents, contractors, or subcontractors of PHI received in connection with Services, the same restrictions and conditions on the *'use'* and *'disclosure'* of PHI that are set forth in this Agreement; such agreement or contract shall comply with 45 CFR § 164.314.
- 4.2 Business Associate shall ensure compliance with this Agreement by its *'workforce'* and *'subcontractors.'*
- 4.3 Business Associate shall adopt privacy, security and breach notification policies and procedures that are consistent with the requirements of HIPAA as applicable to Business Associate.
- 4.4 Business Associate shall implement, maintain and use *'administrative safeguards,'* *'physical safeguards'* and *'technical safeguards'* ("Safeguards") that reasonably and appropriately protect the confidentiality, integrity and availability of PHI as required by 45

CFR Part 164 Subpart C (“Security Rule”) in the same manner that those requirements apply to Health Plan pursuant to 45 CFR § 164.504, and ensure that PHI is not ‘used’ or ‘disclosed’ except as provided for by HIPAA and by this Agreement.

- 4.5 Business Associate shall protect against any reasonably anticipated threats or hazards to the security or integrity of such information, as required by 45 CFR § 164.306.
- 4.6 Business Associate shall prevent, detect, contain and correct against any reasonably anticipated uses or disclosures unpermitted by this Agreement, as required by 45 CFR § 164.306 and § 164.308.
- 4.7 Business Associate shall report to Health Plan any ‘use’ or ‘disclosure’ of PHI, including by its employees, agents, contractors, or subcontractors, that is not provided for by HIPAA or by this Agreement and shall report to Health Plan any breach of unsecured PHI as required by 45 CFR § 164.410, and any successful ‘security incident’ of which it becomes aware.
- 4.8 Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a ‘use’ or ‘disclosure’ of PHI by Business Associate in violation of the requirements of this Agreement or of any ‘security incident’ of which it becomes aware.
- 4.9 In accordance with HIPAA, Business Associate shall make available to Health Plan, in the time and manner designated by Health Plan, PHI that is contained in ‘designated record sets.’ At Health Plan's request, the PHI shall be made available to Health Plan or as directed by Health Plan, to an ‘individual’ in order to meet the requirements under 45 CFR § 164.524. If the ‘individual’ requests an electronic copy of the information, Business Associate must provide Health Plan with the information requested in the electronic form and format requested by the ‘individual’ and/or Health Plan if it is readily producible in such form and format; or, if not, in a readable electronic form and format as requested by Health Plan.
- 4.10 Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for Health Plan to respond to a request by an ‘individual’ for an accounting of disclosures, and at Health Plan’s request, to make available the information necessary to provide an accounting of disclosures of PHI as provided for in HIPAA. Health Plan acknowledges and agrees that neither this Agreement nor the Contract requires Business Associate to make any disclosure for which an accounting would be required under HIPAA.
- 4.11 At Health Plan’s request, Business Associate shall make available PHI in its possession or under its control in ‘designated record sets’ for amendment, and shall incorporate any amendments to PHI in accordance with the requirements of the Privacy Rule and any instructions provided by Health Plan.
- 4.12 Business Associate shall follow any written instructions received from Health Plan with respect to restricting the ‘uses’ and ‘disclosures’ of certain PHI. Business Associate shall ensure that the PHI is not ‘used’ or ‘disclosed’ in a manner that would violate the restriction, unless otherwise directed by Health Plan.
- 4.13 When necessary to accommodate ‘individuals’ reasonable requests for ‘confidential communications,’ Business Associate shall communicate with an ‘individual’ regarding

his/her PHI only in the alternative manner or at the alternative location instructed by Health Plan, unless otherwise directed by Health Plan.

- 4.14 Upon termination, cancellation, expiration, or other conclusion of this Business Associate Agreement, Business Associate shall, after consultation with Health Plan and in accordance with Health Plan's determination, return to Health Plan or destroy (after obtaining Health Plan's permission) all PHI, in whatever form or medium (including in any electronic medium under Business Associate's custody or control) that Business Associate (or its agents, contractors, or subcontractors) created or received for or from Health Plan, including all copies of and any data or compilations that allow identification of any '*individual*' who is a subject of the PHI. Business Associate will identify any PHI that Business Associate (or its agents, contractors, or subcontractors) created or received for or from Health Plan that cannot feasibly be returned to Health Plan or destroyed. If, at the termination of the Business Associate Agreement, the Parties agree that returning or destroying PHI is not feasible due to state or federal law or regulatory requirements applicable to the Business Associate and Health Plan, or due to Business Associate's record retention policies, Business Associate shall extend the protections of the Business Associate Agreement to such PHI, and will limit its further '*uses*' or '*disclosures*' of that PHI to those purposes that make return or destruction of that PHI impractical or impossible. Health Plan hereby acknowledges and agrees that infeasibility includes Business Associate's need to retain PHI for purposes of complying with its work product documentation standards.
- 4.15 For purposes of determining Health Plan's compliance with the Privacy Rule or this Agreement, Business Associate shall make available to Health Plan or the Secretary of HHS (or its agents) the Business Associate's internal practices, books and records relating to the '*use*' and '*disclosure*' of PHI in connection with Services, in a time and manner designated by Health Plan or the Secretary.
- 4.16 If Business Associate accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses '*unsecured protected health information*' (as defined in 45 CFR 164.402 and in HITECH Section 4402 (h)), it shall, immediately following the discovery of a '*breach*' of such information, as defined by HIPAA, notify Health Plan of such breach. Such notice shall include:
- (1) The identification of each '*individual*' whose '*unsecured protected health information*' has been, or is reasonably believed by Business Associate to have been, accessed, acquired or disclosed during such '*breach*;'
 - (2) A brief description of what happened, including the date(s) of the '*breach*' and discovery of the '*breach*;'
 - (3) A description of the type of '*unsecured protected health information*' that was involved in the '*breach*;'
 - (4) A description of the investigation into the '*breach*,' mitigation of harm to the individuals, and protection against further breaches;
 - (5) The results of any and all investigation performed by Business Associate related to the '*breach*;' and

- (6) Contact information of the most knowledgeable individual for Health Plan to contact relating to the ‘breach’ and its investigation into the ‘breach.’
- 4.17 Health Plan has elected to delegate to Business Associate the provision of the HITECH Security Breach services described in Attachment 1, as allowed by HITECH and any subsequent regulation or guidance from HHS.
- 4.18 Business Associate represents that, if applicable, it has policies and procedures in place designed to detect, prevent and mitigate the risk of Identity Theft to comply with the Federal Trade Commission's Identity Theft Prevention Red Flags Rule (16 CFR § 681.2).
- 4.19 **Business Associate shall maintain or cause to be maintained sufficient insurance coverage as shall be necessary to insure Business Associate and its employees, agents, representatives or subcontractors against any claim or claims for damages arising under this Business Associate Agreement. Such insurance coverage shall apply to all services provided by Business Associate or its agents or subcontractors and shall be sufficient to cover acts or omissions of its agents or subcontractors in the performance of the Contract and pursuant to this Business Associate Agreement. Business Associate shall defend, indemnify, save and hold harmless Health Plan and all other parties identified in the Indemnification and Liability Insurance Article of the Contract to the full extent required by that Article of the Contract, and including indemnification for reasonable attorney’s fees and costs, administrative penalties and fines, costs expended to notify participants and/or to prevent or remedy possible identity theft, financial harm, reputational harm, or any other claims related to a breach incurred as a result of, or arising directly or indirectly out of or in connection with any act or omission of Business Associate, its employees, agents, representatives or subcontractors, under this Business Associate Agreement, including, but not limited to negligent or intentional acts or omissions. This provision does not replace or supersede the Contract’s insurance requirements but is intended to be read in conjunction with them. The indemnification obligation of Business Associate shall survive termination of this Agreement.**
- 4.20 In addition to HIPAA, Business Associate shall comply with all applicable state and federal security and privacy laws.
- 4.21 In the event that Business Associate transmits or receives any Covered Electronic ‘Transaction’ on behalf of Health Plan, it shall comply with all applicable provisions of the Standards for Electronic Transactions Rule to the extent required by law.
- 4.22 Business Associate agrees that it will not receive remuneration directly or indirectly in exchange for PHI without authorization unless an exception under 13405(d) of HITECH applies.
- 4.23 Business Associate agrees that it will not receive remuneration for certain communications that fall within the exceptions to the definition of ‘Marketing’ under 45 CFR § 164.501 unless permitted by HITECH.
- 4.24 Business Associate agrees that it will not use or disclose ‘genetic information’ for underwriting purposes, as that term is defined in 45 CFR § 164.502.
- 4.25 The safeguards set forth in this Agreement shall apply equally to PHI, confidential and personal information. “Personal information” means an individual’s first name or first

initial and last name in combination with any one or more of the following data elements, if the name and data elements are not encrypted: (a) social security number; (b) driver's license number or government-issued identification number; or (c) account number or credit or debit card number in combination with any required security code, access code or password, that would permit access to a person's financial account; provided, however, that "personal information" shall not include publicly available information that is lawfully made available to the public from the federal, state or local government.

SECTION V. OBLIGATIONS OF HEALTH PLAN

- 5.1 Health Plan shall not request Business Associate to 'use' or 'disclose' PHI in any manner that would not be permissible under HIPAA if done by Health Plan.
- 5.2 Health Plan shall notify Business Associate of limitation(s) in its notice of privacy practices in accordance with 45 CFR Section 164.520, to the extent such limitation affects Business Associate's permitted 'uses' or 'disclosures.'
- 5.3 Health Plan shall notify Business Associate of changes in, or revocation of, permission by an 'individual' to 'use' or 'disclose' PHI to the extent such changes affect Business Associate's permitted 'uses' or 'disclosures.'
- 5.4 Health Plan shall notify Business Associate of restriction(s) in the 'use' or 'disclosure' of PHI that Health Plan has agreed to in accordance with 45 CFR Section 164.522, to the extent such restriction affects Business Associate's permitted 'uses' or 'disclosures.'

SECTION VI. TERMINATION OF AGREEMENT

- 6.1 Upon Health Plan's knowledge of a material breach of this Business Associate Agreement (or its agents, employees, contractors, and subcontractors), Health Plan shall either:
 - (1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Agreement if Business Associate does not cure the breach or end the violation within the time period specified by Health Plan; or
 - (2) Immediately terminate this agreement if Business Associate has breached a material term in this Agreement and cure is not possible; or
 - (3) If neither termination nor cure is feasible, report the violation to the Secretary of HHS.
- 6.2 The Parties agree that if Health Plan terminates this Agreement pursuant to this section, it shall also terminate all provisions of the Contract for Services that relate to Business Associate's 'use' or 'disclosure' of PHI, and Health Plan shall have the discretion to terminate the Contract for Services in its entirety and pursue all remedies available under the Parties' Contract.

SECTION VII. NOTICES

Any notice or report to be given pursuant to this Agreement shall be sent to the persons listed below in accordance with Section 2.13 of this Agreement.

Covered Entity:

Employees Retirement System of Texas
P.O. Box 13207
Austin, Texas 78711-3207
Attn: Porter Wilson, Executive Director
Email: porter.wilson@ers.texas.gov

cc: Paula A. Jones, Deputy Executive Director and General Counsel
Email: paula.jones@ers.texas.gov

Business Associate:

ImageNet Consulting, LLC
11100 Metric BLVD suite 600
Austin, TX. 78758

THIS SPACE INTENTIONALLY LEFT BLANK.

SIGNATURE PAGE TO FOLLOW.

IN WITNESS WHEREOF, the Parties have executed this Business Associate Agreement as of the day and year written below.

BUSINESS ASSOCIATE

By: *Travis Reeves*

Printed Name: _ Travis Reeves

Title: _Director of SLED Solutions

Date: __8.10.20_____

**EMPLOYEES RETIREMENT
SYSTEM OF TEXAS**

By: _____

Porter Wilson

Executive Director

Date: 2.11.2021_____

ATTACHMENT 1

DELEGATION OF HITECH BREACH NOTIFICATION

The following Health Information Technology for Economic and Clinical Health Act (“HITECH”) Security Breach services will be provided by Business Associate as indicated by Covered Entity in the Business Associate Agreement, as allowed by HITECH and any subsequent regulation or guidance from the HHS:

1. Investigate any unauthorized access, use, or disclosure of Health Plan participant protected health information (“PHI”).
2. Determine whether there is a significant risk of an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of any Health Plan participant’s PHI as provided for in HITECH.
3. Determine whether the incident falls under any of the HITECH Security Breach notification exceptions.
4. Document and retain each HITECH Security Breach risk assessment and exception analyses, and make this information available to Health Plan participants upon request.
5. Provide Health Plan with written notification that describes the HITECH Security Breach incident in detail including a list of the impacted participants and/or a copy of a participant notification.
6. After notice to and consultation with Health Plan, notify each Health Plan participant impacted by the HITECH Security Breach by first class mail, or such other notification method permitted under HITECH, within the applicable statutory notification period, and provide toll-free numbers to the impacted participants in order to handle any participant questions regarding the incident. The notification will include the following:
 - a. A brief description of the incident, including the date of the Security Breach and the date it was discovered;
 - b. A description of the types of PHI involved in the Security Breach (i.e., name, birth date, home address, account number, Social Security Number, etc.);
 - c. The steps that individuals might take to protect themselves from potential harm; and
 - d. A brief description of what the Business Associate is doing to mitigate the harm and to avoid further incidents.
7. Provide a substitute notice, as described in HITECH, to impacted participants if there is insufficient mailing address information.
8. Maintain a log and submit to HHS an annual report of Security Breaches that impact fewer than 500 participants.

9. After notice to and consultation with Health Plan, notify HHS within the time required in HITECH or regulations pertaining thereto in the event the Security Breach impacts more than 500 individuals.
10. After notice to and consultation with Health Plan, notify media when required under HITECH or regulations pertaining thereto, subject to approval by Health Plan, which approval shall not be unreasonably withheld.

The above listed HITECH Security Breach services may be changed from time to time by Business Associate as necessary, after notice to and consultation with Health Plan, and as required to maintain compliance with HIPAA, HITECH, HHS regulation and/or HHS guidance.

DATA SECURITY AND BREACH NOTIFICATION AGREEMENT

All capitalized terms not defined in this Data Security and Breach Notification Agreement (“**Agreement**”) shall have the meaning ascribed to them in the Statement of Work and DIR Contract No. 4159 (“**Contract**”) between the Employees Retirement System of Texas (“**ERS**”) and ImageNet Consulting, LLC (“**CONTRACTOR**”).

Article 1. Purpose

- 1.1 To ensure continued security for ERS, its members, annuitants, retirees, participants, alternate payees and beneficiaries (collectively “**Members**”) and their respective Personal Data (as hereinafter defined), and to mitigate the risk of identity theft and fraud, CONTRACTOR agrees to be bound by the provisions contained in this Agreement.

Article 2. Specific Requirements

- 2.1 CONTRACTOR, including its affiliates, subsidiaries, representatives, officers, directors, principals, employees, agents, assigns and any subcontractors and independent contractors (“**Agents**”), as a condition of handling Members’ personally identifying and / or sensitive personal information and, if applicable, protected health information (“**PHI**”) (together, “**Personal Data**”) must annually, or more frequently upon request of ERS, issue certificates of compliance with this exhibit to ERS and permit ERS to initiate independent audits to verify compliance with same.
- 2.2 All Personal Data must be processed fairly and lawfully, according to the laws and regulations of the United States of America and the state of Texas. CONTRACTOR shall comply with the Privacy Act of 1974, Computer Matching and Privacy Protection Act of 1988, Texas Business and Commerce Code, ch. 521 and information security standards as outlined in Title 1, Texas Administrative Code, § 202. Further, CONTRACTOR shall comply with all applicable federal and state laws and regulations pertaining to the handling and use of Personal Data. In the event of a conflict between applicable laws, the Contract and this Agreement, the strictest provision or provisions offering protections to ERS and its Members shall apply.
- 2.3 The amount of Personal Data collected must be adequate, relevant and not excessive in relation to the purposes for which it is collected or for which it is further processed. If applicable, PHI must be collected only for purposes consistent with what is communicated to the Member and not further processed in a way incompatible with those purposes. All other Personal Data must be collected only for purposes as necessary for CONTRACTOR to perform and fulfill its obligations under the Contract and not further processed in a way incompatible with those purposes. Further processing of such Personal Data for historical, statistical or other business purposes is not incompatible with the original purpose, provided it is permitted under the Contract and the further processing includes adequate additional controls protecting the rights of the Member.
- 2.4 If CONTRACTOR serves as a recordkeeper for ERS or collects data on behalf of ERS, all Personal Data must be accurate and complete, and where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data that is inaccurate or incomplete, keeping in mind the purposes for which it was collected or for which it is further processed, is definitively erased or corrected in accordance with applicable law.
- 2.5 If CONTRACTOR did not execute a Business Associate Agreement (“**BAA**”) in connection with the Contract, but CONTRACTOR subsequently receives or handles any PHI, CONTRACTOR agrees to immediately notify ERS. ERS will then determine, in ERS’ sole discretion, whether CONTRACTOR must execute a BAA to address the privacy, security and breach notification requirements related to PHI. If applicable, CONTRACTOR agrees to act in good faith and to cooperate in the execution of a BAA.

- 2.6 CONTRACTOR shall maintain industry-accepted standards, such as those recommended by the National Institute of Standards and Technology (NIST), and shall incorporate other applicable state and federal laws and regulations regarding the confidentiality, integrity, accessibility and availability of Personal Data, including, but not limited to, maintenance of disaster recovery and business continuity plans. CONTRACTOR agrees to allow ERS to view these standards and plans upon request onsite at ERS' premises.
- 2.7 CONTRACTOR shall maintain computer files containing Personal Data in a secure, hardened facility which provides environmental and access controls. All computer files containing Personal Data, including, but not limited to, duplicate or backup copies, shall be encrypted while at rest and in transit. Additionally, all mobile devices, including, but not limited to, laptop computers, and external storage devices which contain, process or interact with ERS data, including, but not limited to, Personal Data, shall be encrypted at all times.
- 2.8 Except as specifically permitted by ERS, Personal Data must not be kept in a form that permits identification of Members for any longer than is necessary for the purposes for which the data was collected or for which it is further processed. For example, this can be implemented with linked separate files that contain identification information and related sensitive information, respectively.

Article 3. Processing Confidentiality and Security

- 3.1 Personal Data shall not be made available to or viewed by any person or entity (including any Agent of CONTRACTOR), in any fashion, no matter what technology is employed, at any location outside the fifty (50) states of the United States of America. Access to Personal Data for purposes of this requirement occurs whenever it is possible to view Personal Data from outside the United States, whether or not the Personal Data is actually sent out of the United States or is actually viewed by someone outside the United States.
- 3.2 When building, testing, enhancing and maintaining processing systems that contain, or will contain, Personal Data, developers must not use actual Personal Data. Instead, they must use fictional or sanitized data that preserves the essential characteristics of the Personal Data, but that does not relate to identifiable individuals. In emergency situations where processing with actual Personal Data is required, use of such information may be permitted only if security procedures are approved in advance, in writing, by ERS' Executive Director, Deputy Executive Director and General Counsel and Information Security Officer.
- 3.3 All authentication access to processing systems and networks containing Personal Data must be logged so that access attempts to systems and networks containing Personal Data can be traced to a specific user. CONTRACTOR is responsible for monitoring and following up on potential security-relevant events.
- 3.4 When no longer needed, or as required by applicable state or federal law or the Contract, all copies of Personal Data, including, but not limited to, copies on backup tapes, must be irreversibly destroyed according to standards and procedures as provided in the Contract and applicable law. A document describing the Personal Data destroyed, the reasons for such destruction, date and manner thereof and who performed such destruction must be prepared for each destruction process and promptly submitted to ERS. Permission to destroy Personal Data may be granted only by ERS, and only if all legal retention requirements and related business and auditing purposes have been met, and as consistent with the terms of the Contract. In the event there is any litigation or investigative proceedings related to the Personal Data or CONTRACTOR's performance under the Contract or this Agreement, then the Personal Data must be retained during the pendency of such litigation or investigative proceedings.

Article 4. Data Breach Monitoring and Notification

- 4.1 CONTRACTOR must take proactive steps to monitor for breaches of system security, including, but not limited to, acquisition, access, use or disclosure of Personal Data (each, a "**Notification Event**"). In the event of such a Notification Event, CONTRACTOR must notify ERS immediately, but in any event within 24 hours from the time the Notification Event is discovered or reasonably should have been discovered with the exercise of reasonable diligence, whichever is earlier. The primary contacts for notification at ERS are the Deputy Executive Director and General Counsel and Information Security Officer. At any time upon request of ERS, CONTRACTOR must notify, at CONTRACTOR's expense, the affected Member(s), including those Members reasonably believed to have been affected, as quickly as possible, but in any event within 72 hours from the time the Notification Event is discovered, unless requested to withhold notification by law enforcement or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- 4.2 If CONTRACTOR is required to notify at one time more than 10,000 Members of a Notification Event, pursuant to applicable law, CONTRACTOR shall also notify, without unreasonable delay, all consumer reporting agencies that maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices.
- 4.3 In addition to indemnification of the Indemnified Parties pursuant to the Contract and any criminal or civil penalties, including injunctive relief, that may apply, **CONTRACTOR AGREES TO DEFEND, INDEMNIFY, SAVE AND HOLD HARMLESS, AND TO PROVIDE, AT CONTRACTOR'S SOLE COST AND EXPENSE, ONE (1) YEAR OF CREDIT MONITORING SERVICE TO, ANY MEMBER(S) WHOSE PERSONAL DATA HAS BEEN DISCLOSED PURSUANT TO A NOTIFICATION EVENT.** ERS will designate the vendor that will provide the credit monitoring service.

IN WITNESS WHEREOF, the Parties have executed this Agreement to be effective upon execution by both Parties.

[CONTRACTOR]

EMPLOYEES RETIREMENT
SYSTEM OF TEXAS

By: Travis Reeves
Name: Travis Reeves_____

By: Porter Wilson
Porter Wilson_____

Title: Director of SLED Solutions____

Executive Director

Date: 8.10.20_____

Date: 2.11.2021_____

STATE OF TEXAS §
 §
COUNTY OF TRAVIS §

**CONFIDENTIALITY AND
NONDISCLOSURE AGREEMENT**

ImageNet Consulting, LLC with its principal place of business at 19001 N Heatherwilde Blvd Building 1 Ste. 100, Pflugerville, TX 78660 (“**Contractor**”), desires to work with the Employees Retirement System of Texas, whose place of business is located at 200 E. 18th St., Austin, Texas 78701 (“**ERS**”), for purposes of providing printer fleet management services as set forth in ERS’ Statement of Work (“**Services**”), to be purchased by ERS pursuant to ERS’ Purchase Orders, including under DIR Contract No. DIR-TSO-4159 and any renewals or replacements thereof, as applicable, between the State of Texas, acting by and through the Department of Information Resources and Contractor (“**Contract**”).

Although ERS is subject to the Texas Public Information Act, Tex. Gov’t Code Ann., ch. 552 (West 2012 & Supp. 2014), ERS maintains documents and information that are considered confidential by ERS and/or by law (“**Confidential Information**”). The Confidential Information includes, but is not limited to, any and all discussions and communications with ERS and any and all information and documentation provided by ERS, including, but not limited to, information related to ERS’ network system architecture and infrastructure; ERS’ existing firewall environment and firewall configuration; and information pertaining to ERS’ members, annuitants, retirees, participants, alternate payees and beneficiaries (“**Members**”) in any program or retirement system administered by ERS. Further, the Confidential Information also includes, but is not limited to, records and confidential or protected health information (“**PHI**”), as PHI is defined by the privacy regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”) of any or all Members.

Contractor agrees that all Confidential Information provided and/or made available to Contractor and/or its Related Parties (as hereinafter defined) by ERS and/or accessed by Contractor and/or its Related Parties (whether accessed onsite at ERS or remotely) must remain confidential and subject to release or disclosure only by prior written consent of ERS, except as provided in this Confidentiality and Nondisclosure Agreement (“**Nondisclosure Agreement**”). Contractor additionally acknowledges and agrees that ERS will require execution of this Nondisclosure Agreement as a precondition to commencement of the Services.

ERS and Contractor (sometimes hereinafter referred to as “**the parties**”) agree that the consideration underlying this Nondisclosure Agreement is contained in the Contract, including ERS’ Purchase Orders.

The parties hereby further agree as follows:

1. The Confidential Information is the exclusive property of ERS and shall be properly safeguarded and kept confidential as required by this Nondisclosure Agreement and any and all other applicable Texas and federal laws and regulations including, but not limited to, Tex. Gov’t Code Ann. §§ 552.0038, 552.110, 552.143, 615.045, 803.402, 815.503, 840.402 (West 2012) and 2054.077 (West Supp. 2014); Tex. Ins. Code, § 1551.063 (West Supp. 2014);

HIPAA, the HIPAA Privacy Rule, the HIPAA Security Rule and the Health Information Technology for Economic and Clinical Health Act (“**HITECH**”). Contractor warrants and represents that (a) it has systems, measures and procedures in place to safeguard and maintain, and to cause its employees, temporary workers, officers, directors, principals, affiliates, agents, assigns, independent contractors, subcontractors, successors or any other related person or entity (“**Related Parties**”) to safeguard and maintain, the confidentiality of the Confidential Information at all times; and (b) Contractor and the Related Parties shall safeguard and maintain the confidentiality of the Confidential Information at all times in accordance with this Nondisclosure Agreement and applicable law.

2. The Confidential Information may be used by Contractor and/or its Related Parties only as necessary to perform the Services for which such Confidential Information is provided to Contractor by ERS. Contractor may not assign or subcontract any of its obligations under this Nondisclosure Agreement.
3. Contractor and the Related Parties shall not copy, reproduce, distribute, disseminate, sell, assign, release, convey, give away or otherwise provide the Confidential Information to any person or entity without ERS’ prior written consent and except as is absolutely necessary for the Services. This entire paragraph shall survive any termination, expiration, renewal, extension or amendment of this Nondisclosure Agreement.
4. Contractor warrants and represents that any Confidential Information transmitted by it or the Related Parties shall be disseminated in an encrypted fashion readable to ERS.
5. Contractor warrants and represents that Contractor and the Related Parties shall not in any manner contact ERS’ Members or make use of the Confidential Information to contact ERS’ Members unless directed to do so by ERS.
6. Contractor and the Related Parties may not retain any copies, electronic or otherwise, of the Confidential Information.
7. This Nondisclosure Agreement and the parties’ performance of same and all matters in connection with the relationship of the parties shall be governed by and construed and performed in accordance and conformity with the laws of the state of Texas without regard to conflicts of law provisions. Subject to and without waiving ERS’ or the state of Texas’ sovereign or official immunity, ERS and Contractor agree and consent to Austin, Travis County, Texas as the proper venue for any court proceedings between the parties, and that a Texas state court sitting in Austin, Travis County, Texas shall have jurisdiction in connection with any action or proceeding arising out of, in connection with or related to the Nondisclosure Agreement or the parties’ relationship. Contractor and/or its Related Parties shall not, at any time, use the Confidential Information in any fashion, form or manner except in Contractor’s capacity as independent contractor to ERS and as described herein. This entire paragraph shall survive any termination, expiration, renewal, extension or amendment of this Nondisclosure Agreement.

8. In addition to any other rights and remedies available to ERS under this Nondisclosure Agreement, at equity or pursuant to applicable statutory, regulatory and common law, the breach of this Nondisclosure Agreement by Contractor and/or its Related Parties shall entitle ERS to immediately terminate the Contract and Contractor's and/or its Related Parties' right of access to and possession of the Confidential Information pursuant to the terms of this Nondisclosure Agreement. In the event that ERS terminates Contractor's and/or its Related Parties' right of access to the Confidential Information, ERS shall provide written notice to Contractor that all Confidential Information made available to Contractor and/or its Related Parties pursuant to this Nondisclosure Agreement, or to which Contractor and/or its Related Parties have been provided access pursuant to this Nondisclosure Agreement, including in each event all copies thereof, must be returned to ERS as soon as reasonably possible after Contractor's receipt of such notice from ERS. This entire paragraph shall survive any termination, expiration, renewal, extension or amendment of this Nondisclosure Agreement.
9. **Due to the sensitive nature of the Confidential Information that ERS is providing to Contractor, Contractor agrees to defend, indemnify, save and hold harmless the state of Texas, its past, present and future officers, departments, employees and agencies, ERS, its past, present and future officers, directors, trustees, employees, attorneys, and agents, from and against any and all damages and claims of contribution and indemnity, any other claims, lawsuits, settlements, liability, judgments, costs, penalties, losses and expenses of whatever nature, kind or description, of any person or entity whomsoever, including, without limitation, interest, court costs, attorney fees, and any measure or type of damages (collectively "Claims, Liability and/or Damages"), resulting from, alleged to result from, in connection with, arising out of, or related to:**
- A. **Any intentional or negligent failure, refusal or inability of Contractor or the Related Parties to meet or comply with any of their obligations under this Nondisclosure Agreement.**
- B. **Any other malfeasance, misfeasance, omission or act of negligence on the part of Contractor and the Related Parties in meeting such obligations, including improperly Disclosing to any person or entity the Confidential Information or for any intentional or malicious act in violation of such obligations.**

This indemnification includes, but is not limited to, any and all Claims, Liability and/or Damages resulting from, alleged to result from, arising out of or in connection with alleged negligence or intentional wrongdoing by Contractor or the Related Parties and all Claims, Liability and/or Damages resulting from, alleged to result from, arising out of or in connection with Contractor's or the Related Parties' failure or inability to comply with applicable Texas and federal laws and regulations. This provision shall not be construed to eliminate or reduce any other indemnification or right which ERS has in law, contract or equity. This obligation to indemnify shall survive any termination, renewal or amendment of the Nondisclosure Agreement.

10. Contractor warrants and represents that it has full power and authority to enter into this Nondisclosure Agreement, and that the Nondisclosure Agreement has been duly authorized, executed and delivered by Contractor's authorized officer on behalf of Contractor and constitutes a valid, binding, and legally enforceable agreement of Contractor.
11. **Contractor warrants and represents that it will give immediate notice to ERS of any breach of this Nondisclosure Agreement.**
12. **Any notices required pursuant to this Nondisclosure Agreement shall be given by hand-delivery, facsimile or email to:**
 - A. **Contractor at:**
ImageNet Consulting, LLC
19001 N Heatherwilde Blvd Building 1 Ste. 100, Pflugerville, TX 78660
Attn: Ryan Starks
Telephone: 512.610.2480
Fax: n/a
Email: rstarks@imagenet.com
 - B. **ERS at:**
Employees Retirement System of Texas
P.O. Box 13207
Austin, Texas 78711-3207
Attn: Porter Wilson, Executive Director
Email: porter.wilson@ers.texas.gov
cc: Paula A. Jones, Deputy Executive Director and General Counsel

Fax: (512) 867-3480
Email: paula.jones@ers.texas.gov
13. This Nondisclosure Agreement shall become effective as of the date Confidential Information is first made available to Contractor and/or its Related Parties, and shall survive any termination, expiration, renewal, extension or amendment of the parties' relationship, for whatever reason, and shall survive so long as Contractor and/or its Related Parties have access to or possession of any Confidential Information, including originals, copies or otherwise.

14. Without limiting the obligations of Contractor and/or its Related Parties to comply with the terms of this Nondisclosure Agreement, Contractor agrees that Confidentiality Acknowledgements in the form attached to this Nondisclosure Agreement shall be executed by all persons who work on the Services and/or who have access to Confidential Information.
15. Contractor agrees to monitor the performance of all persons having access to the Confidential Information on its behalf, and to be liable for the actions of all such persons.
16. This Nondisclosure Agreement may be executed and delivered by email; such email delivery shall constitute the final Nondisclosure Agreement of the parties and conclusive proof of such Nondisclosure Agreement. Original signatures may be provided to the parties thereafter.

The authorized representatives of ERS and Contractor hereby execute this Nondisclosure Agreement to be fully effective immediately upon execution by an authorized representative of ERS as set forth below, and by doing so evidence their mutual intent to be legally bound by the terms set out above.

IMAGENET CONSULTING, LLC

By: Travis Reeves
 Printed Name: Travis Reeves

Title: Dir of SLED Solutions and Enterprise Accounts

Date: 3.5.21

EMPLOYEES RETIREMENT SYSTEM OF TEXAS

By: Porter Wilson
 Porter Wilson
 Executive Director

Date: 3/9/2021