Texas Department of Information Resources
DIR Contract Number: DIR-CPO-4407
Appendix D Service – Support Agreement

Neubus, Inc.
2300 Greenhill Drive, Bld 9, Ste 900
Round Rock, TX 78664
512-833-6197
www.neubus.com

Introduction:
For the last 18 years, Neubus, Inc. has continued to fine-tune the described services and support to give our Customers all that they need and all that they want from Neubus; a true “one-stop shopping” experience. Neubus has utilized this tried and true approach to ensure our DIR eligible Customer services are restored no matter what.

In short, Neubus will do what it takes to secure our Customers’ satisfaction and we’ve found that this philosophy works best for our Customers.

The Services outlined below are available by this Appendix D Services-Support Agreement to DIR Contract Number DIR-CPO-4407 to all existing and potential DIR eligible Customers. All Services provided shall be in accordance with Appendix C Pricing Index for DIR Contract Number DIR-CPO-4407.

A. Document Imaging Services/Solutions (DIS)

1. Document Conversion
2. Preservation and Archive Scanning and Imaging
3. Document Preparation
4. Indexing and Formatting
5. Digital Retention, Storage and Hosting
6. Microfiche and Digitization Imaging
7. Image Enhancement
8. ICR/OCR/OMR
9. Interface with Customer System

B. ECM Managed Services Solution

1. Document Conversion
2. Records Management and Storage
3. Transactional Content Management
4. Social Content Management
5. Software as a Service for Video, Mobility, Social, and Cloud Platforms
6. Archiving
7. Imaging
8. Business Process Management
9. Records Management
10. Document Management
11. Web Content Management
12. Project Management (Related Service)

Continued on Next Page

I. Customer Service

Technical Support/Help Desk Service

Defect monitoring, tracking and resolution is performed using Neubus' Support Management Services (SMS), an online enterprise-grade ticketing system that enables Neubus staff to intelligently and efficiently manage tasks and issues submitted by Customers.

The online ticketing system manages key tasks such as problem identification, prioritization, assignment, investigation, resolution, and notification, as well as automatic ticket escalation.

SMS will serve as the primary vehicle by which all DIR customer-related problems, issues, or defects are reported as identified during the DIR customers' user acceptance reviews of Neubus' service deliveries. SMS tickets are monitored and tracked constantly by Neubus customer support teams for the timely resolution and closure of all DIR customer-submitted tickets. With Neubus senior management conducting weekly internal reviews of open tickets status, Neubus can ensure support tickets are meeting response and resolution criteria.

The advantages of using this system for the resolution of all issues include the following:

- At the point that the DIR customer initiates a SMS ticket, information is immediately transmitted to the appropriate members of the Neubus support team. For a given level of severity, the system is designed to escalate through the Neubus organization if an appropriate response is not made by one of the primary persons contacted in an appropriate timeframe. See table below.
- Use of the SMS system ensures that there is complete visibility and ease of tracking as it relates to the resolution of a problem.
- The system allows Neubus personnel to manage, respond to, and resolve all issues that need to be worked in a more expeditious manner than if any other communication vehicle were being used (e.g., email). This is because all problems are centrally managed in one system, allowing the Neubus team to be able to more efficiently track, respond to, and solve them.

	Criteria	Target Response Time	Target Resolution Time	Contact
Severity I	Complete work stoppage for all users (critical function such as retrieval), or all workstations disabled. Executive support. No work can be performed.	2 business hours	24 calendar hours	Open ticket on Online Ticketing System Automatic ticket escalation with SMS and email notification; or call to helpdesk
Severity II	Partial work stoppage: major functions or some workstations disabled. Some work can be performed.	8 business hours	5 business days	Open ticket on Online Ticketing System Automatic ticket escalation with SMS and email notification
Severity III	Partial work stoppage: minor functions disabled. Most work can be performed.	16 business hours	20 business hours	Open ticket on Online Ticketing System Automatic ticket escalation with SMS and email notification
Severity IV	Suggestions			support@neubus.com

Issues related to Neubus-defects will be resolved without charge. If there are issues that are determined to not be Neubus defects, then at Neubus' discretion the DIR customer may incur technical support charges in accordance with Appendix C Pricing Index of DIR Contract Number DIR-CPO-4407.

Remedy

Neubus will correct, at its expense, digital imaging defects that deviated from project specifications, including deficiencies in image quality caused by Neubus processing. Neubus will rework any assignments that have an error rate exceeding the AQL, "customer's tolerance for errors", at no charge to the DIR customer. As part of the Neubus imaging quality control program, Neubus will review all images for quality and adherence to the AQL.

Neubus will make corrections for a period of twelve (12) months from delivery, unless otherwise agreed-to with the DIR Customer.

II. Software Support and Hardware Maintenance

Software Support

Neubus develops and releases software enhancements on a semi-annual or annual basis. Each release is provided to Customers free of charge. Customer-specific software configuration changes related to a release (or changes requested by the Customer as a result of having enhanced functionalities due to a release) will be billed to the Customer as programming support and/or technical support in accordance with Appendix C Pricing Index of DIR Contract Number DIR-CPO-4407. Customers who participate in Appendix D to DIR Contract Number DIR-CPO-4407, Neubus' Loyalty Rewards Program may apply their loyalty rewards credits (LRC) to offset those professional services charges. Please refer to Appendix C-1 for Neubus' Loyalty Rewards Program for further information.

Software updates may be deployed by Neubus to address vulnerabilities to the system. These represent potential threats that are flagged during Neubus' robust and continuous security monitoring and penetration testing. These fixes or patches are provided to Customers free of charge.

Hardware Maintenance

All server hardware is provided by Neubus.

Services are maintained at no cost to Customers. Neubus also provides desktop scanning hardware as needed to Customers as part of our "one-stop shopping" services. Neubus will provide all required hardware maintenance for the desktop scanners that have been deployed to the Customers' sites. This maintenance covers replacement of the rollers once they have reached their recommended usage limit (based on the page counts tracked for each scanner), and all other major components of the hardware.

Customers with Neubus' desktop scanning hardware are required to perform maintenance tasks on a daily basis such as cleaning the rollers, lens, and scanner glass, etc. using appropriate cleaning materials to ensure optimal scanner performance. Customers are responsible for supplying such standard consumables such as compressed air and alcohol pads to sufficiently clean the hardware.

Should an issue arise with the desktop scanner that Neubus support is unable to resolve online and/or over the phone within the stated resolution criteria, Neubus will either dispatch technical support to troubleshoot the problem or send a replacement scanner within 24 hours.

III. Security

SOC 2/3 Type 2 Certification

Neubus exercises continuous process improvement and vigilance to assess risks, monitor and test security protection. Neubus has undergone System and Organization Controls (SOC) 2 Type 2 compliance audit and has the SOC 2 and SOC 3 reports resulting from the audit. Like the SOC 2 report, the SOC 3 version will provide the Customer a description of our system and is focused on our pre-defined, standardized benchmarks for controls related to Security, Availability, Processing Integrity, and Confidentiality. The SOC 3 report contains the auditor's opinions and is suited for public dissemination. Neubus' SOC 3 report with our SOC 2 Type 2 audit shows that Neubus has the highest level of compliance and assurance of operational excellence. Our full SOC 2 report can be provided after receipt of a signed non-disclosure agreement (NDA) if the Customer wishes to review the auditor's testing and results.

Security Monitoring

In accordance with Neubus' Security Policy, Neubus employs various network and server monitoring technologies to protect all Neubus computing systems, network infrastructure, and most importantly, Customer data. These technologies include anti-virus software, firewalls, intrusion protection and intrusion detection systems, vulnerability management systems, and server and application monitoring systems.

Confidentiality of any information gathered as a result of monitoring will be maintained at all times. Any access to information obtained through security monitoring is limited to select, designated Neubus staff.

Physical Storage

In performance of a project work order (including at least 30 Business Days prior to production start as well as at least 30 Business Days post final output acceptance), physical boxes will be securely stored (without storage fees) while the source materials are in Neubus' custody waiting to undergo Neubus conversion, are currently in conversion processing, or have completed Neubus' conversion services. All Customer source materials are inventoried/catalogued prior to placement and storage within Neubus' code-compliant (NFPA 2017) concrete facility structures complete with security certification, monitoring 24/7/365, strict environmental controls, and RFID asset tracking and management. Neubus maintains secure areas for both work and storage that offer optimal environmental conditions for Customer source and archival materials. This includes providing physical storage according to stringent standards for temperature, humidity, light, air quality, gas fire suppression, UV light exposure limits, etc., as specified by project requirements.

Neubus facilities are inspected by the City of Austin Fire Marshall and any discrepancies are noted and immediately corrected. Neubus' fire detection system consists of heat sensors throughout the facility as well as sensors in Neubus' HVAC units.

Neubus' physical security measures include the following building access controls:

1) The facility entrances are controlled by both physical key locks and smart access card technology. Offices and file cabinets are controlled with key locks. Loading doors remain padlocked at all times unless in use. All personnel doors are electronically locked during business hours and require badge access. Personnel doors are additionally key locked during non-business hours. Keys to the facility are only issued to operations managers and shift supervisors who are responsible for opening and closing

facilities. At the beginning of a shift, the shift supervisor completes a physical inspection of all doors to ensure that there has not been any attempt to bypass security or lack of control on these locks that are deemed critical to security at the facility. Any abnormal situations found are reported to Production Operations Management. All access points are monitored by a security company during non-business hours.

2) The entire facility is controlled by smart card readers. Neubus issues smart access cards only to authorized personnel who perform regular job functions in the facility. Secure areas are protected by door access badges. Customer material is stored behind at least two doors requiring badge access. The document and preparation and scanning area is protected by additional smart card readers that require a higher level of access authorization. Such access is only granted to personnel who perform regular job functions in the document preparation and scanning area.

3) Neubus' security system monitors all access points. Facility entrances are electronically monitored to ensure closure. Neubus' security system provides automatic record of badge access used (authorized and denied) during business hours so employee movements can be tracked through secure areas and building entry. When needed, both Production Operations Management and the assigned security personnel will review the security log. This log allows security administration including Neubus' senior management to respond to and track any problem that arises. Examples of problems are: badge access reader failure, door closure problems, security system failures, and door propped open.

4) The Production Operations Management maintains a current listing of personnel who are authorized access to controlled areas. The access list includes production staff and personnel who have requirements to provide technical and managerial support, and a select few of the onsite vendors. Only Production Operations Management will submit addition or deletion of entries into the access list. All access must be obtained through Production Operations Management based upon job requirements with management approval. Employees are allowed access only after successfully completing background checks and an IT ACC access control form is submitted by their supervisor and approved by the CTO. Only then can HR update their access card granting unescorted access into secure areas. Employee access is determined by need of access and is dependent on job duties. Production Operations Management and HR work together to update the access list each time an individual's employment or project status changes as well as review the list on a quarterly basis to ensure it kept updated to accurately reflect active employees and the access level authorization(s) of the employees. Building access is immediately revoked for employees who leave Neubus. These employees are required to have an exit interview when badges and access keys are returned. Computer software/hardware access is removed, their logon ID is revoked and login capability is removed for all Neubus and agency project systems.

   Neubus security tracks all logons and attempted logons and will notify Production Operations Management if there is are multiple attempts to logon that failed or any attempted hacking of the Neubus entry system.

5) Security cameras are strategically placed within the production facility to track employee movements. They also provide documentation in case of theft or robbery.

6) Security and Fire Alarm services are maintained to protect against external and environmental hazards. Both systems are monitored. Battery backups and redundant communications are in place for reporting faults. Fire extinguishers are located throughout the facility and are checked monthly.

7) All escorted visitors and equipment repair personnel are required to sign in and out of Neubus facilities via the security tracking log and are identified with a "Visitor Badge". A picture identification (ID) must be presented and identification verified before access is allowed.

The security tracking log will be utilized to track all of the following:

- Who is onsite?
- What company are they with?
- For what reason are they onsite?
- Does the person(s) have clearance to be onsite?
- What type of temporary access badge was issued (level of access)?

Visitors must be escorted at all times and are never allowed access to any work unless accompanied by a Neubus employee. An escort is defined as a Neubus or vendor staff who has received appropriate Customer-specified clearance.

All visitors are required to sign out when leaving the facility for any reason – lunch, break, or completion of their visit. At the end of each security shift, all visitor badges and numbers are accounted for. Any badge not accounted for is noted and the matter referred to Production Operations Management.

Challenge procedures assist personnel in handling visitors without proper identification. If anyone is found on the production floor or anywhere else in the facility without the proper identification, challenge procedures are followed. These procedures are in place for employee safety and the continued integrity of the document and data housed at the facility:

- Escort the person(s) to Production Operations Management.
- Check the access list to see if they are cleared to be onsite and without an escort.
- Find out if they are working on a scheduled maintenance or troubleshooting a current problem.

If the person(s) were not scheduled to be onsite, Production Operations Management escorts them to the lobby immediately. A member of the Operations Team informs a member of management of the current situation. It is up to management whether or not the person(s) should be escorted out of the building. Any and all personnel working at the Neubus facility are required to have an employee badge denoting security clearance areas. Anyone found in an unauthorized area, unless escorted by an authorized employee, will be escorted out to an area they are authorized to access. These occurrences are also reported to Production Operations Management. The requestor must provide the following information to Production Operations Management before access will be provided:

- Full name
- Group or company name
- Areas of access
- Reason for access
- Duration of required access

Personnel not on the secured access list may not be admitted, unless escorted, into controlled areas. A picture ID must be presented and identification verified before access is allowed.

The facility has physically separated containment areas: document preparation and scanning areas within Neubus' facility require a higher level of smart card access authorization granted only to personnel who perform job functions in the document preparation and scanning areas. Neubus will provide secure storage of the DIR customer's source media as well as any output media while in its custody. While being processed, Neubus will maintain all DIR Customer source materials/boxes and output media within the appropriate secured containment areas (e.g. shelving, document prep and imaging area, secured document storage area, etc.).

Electronic Storage

In accordance with Appendix C Pricing Index of DIR Contract Number DIR-CPO-4407, Neubus offers Customers a three-tiered storage service (e.g. online, nearline, and offline) to proactively meet Customer needs. Please contact Neubus for additional information about our three-tiered storage service. Neubus' electronic security measures include the following:

1. Network: Neubus limits any external connectivity to approved connections for which system interconnection agreements exist using Federal Information Processing Standards (FIPS) 140-2 compliant encryption software. Transmission of information is over protocols such as Secure File Transfer Protocol (SFTP) and Secure Shell (SSH) software that are FIPS 140-2 compliant. The network and systems are configured to disallow active ActiveX or .NET and any active code not specifically approved and necessary for completion of the project. Security audit logs are enabled and configured to provide the information needed to monitor system security relevant events. User IDs and passwords are required and configured (e.g., password length and complexity) to fully meet the 1 TAC 10 202 requirements.
2. Encryption: Neubus' encryption processes for data in motion complies, as appropriate, with NIST Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, and/or others which are FIPS 140-2 validated.

   Datalocker encrypted hard drives are used for physical transport of output data. Customer source data and/or production data is stored in servers which are located in secured server rooms controlled by Customer (on-promise) or secured data centers with ISO/IEC 27001, SSAE 16 (SOC 1 Type II), Type 2 AT 101/SOC 2 & 3, PCI DSS, FISMA-High, HIPAA/HITECH compliance. Electronic access to these servers is controlled by firewall and user authentications. When data is accessed outside of a Customer's local area network (LAN), encryption technologies (such as SSH, SSL, AES, etc.) are implemented from encrypted workstations to ensure data transfer security. Only those administrators and servers at Neubus required to update and monitor the server will be allowed SSH (secure shell) access. Source code and image updates are transferred using FIPS 140-2 compliant OpenSSH protocols. Furthermore, authenticated users can only access the Customer source data and/or production data that they are authorized to access based on their roles and/or user IDs. Overall server security is based on NIST SP800-123, Redhat's Security Guide. Specific SSH security configurations, MAC algorithms and ciphers are based on recommendations from nsa.gov, cert.org and nist.org. Neubus uses 2048-bit RSA keys for ssh/scp authentication. Only NIST validated Encryption algorithms are allowed.

   For backup tapes, Neubus relies on hardware encryption (not software encryption) done at the tape library level. This ensures that the tape will not be readable without the hardware encryption server.
3. Data: All data will be appropriately protected and handled, regardless of the format it resides on. Sensitive personally identifiable information (PII), protected health information (PHI), and any other information that may be subject to Government handling and management requirements (Privacy Act, etc.) will be managed so as to prevent unauthorized disclosure. Neubus' encryption processes for data at rest and data in transit are consistent with Criminal Justice Information Services (CJIS) Security

Policy. Digital information stored or transported by Neubus is appropriately encrypted with a FIPS 140-2 compliant application.

Employees are trained and certified for certain production tasks and through Neubus' PCS2, are restricted to the tasks on which they are certified to perform through role-based access controls. This also acts as a mechanism to limit the number of individuals who are authorized to handle a Customer's source documents.

Procedures are established for sanitizing all fixed storage media (e.g., disks, drives) at the completion of the contract and/or before it is returned for maintenance, disposal or reuse. Sanitization procedures include overwriting the media and/or degaussing the media in accordance with the NIST Special Publication 800-88. If media cannot be successfully sanitized it will be returned to the Customer or destroyed.

Hiring, Background Checks and Onboarding of Employees

Neubus will not outsource any part of a DIR customer's project order to a third party.

As part of staffing to meet the needs of the DIR customers' project orders and any additional requirements determined with the participating DIR customers, Neubus will initially draw upon its existing pool of employees and utilize recruitment when needed. All candidates, whether existing employees or new hires, will undergo the prescreening, interview and appropriate background checks

Neubus' HR will play a critical role in organizing the personnel sourcing requirements. HR will meet with the Neubus management, Project Manager, and Production Operations Managements to review the project documentation and assess the personnel needs for project work associated with the DIR customer's project order gaining an understanding of the staffing requirements for the DIR customer's project orders. This involves mapping out each skill set required (prep, scan, index, etc.) and any particular skills being required, skill level (entry level, senior level) and the number of employees required for each function (prep, scan, index, etc.). Once the type of work and number of people are identified, the recruiter will determine the availability of internal Neubus staff to participate in the project and the need to on-board new hires for newly created positions.

The result of meeting with Neubus management will provide the recruiter with the information needed to develop a project staffing matrix and begin staffing the project, and use established recruiting procedures to write position descriptions and requirements if needed.

All candidates, whether existing employees or new hires will undergo the prescreening, interview and background checks as required by Neubus and the DIR customer. Neubus will establish a pool of candidates for the DIR customer's project work and track them as follows:

1. Current employees with the right skill set and level will be asked to update their information in the HR database and will be notified that Neubus is considering them for a project order.
2. Candidates that are already in the HR database will be notified that they are being considered for the project order and asked to review their current application information and to update that information as applicable to reflect their current training programs, certificates, degrees, etc. These candidates will be asked about their availability for work on the project order.
3. New candidates, not currently in the database, will be asked to submit an application using our online web-based application process. This includes: a) completing the application, b) pre-screening work experience questionnaire, c) Capstone Inventory test. The Capstone Inventory Test is based on

O*NET job descriptions. The Capstone Inventory is a comprehensive test of the skills required for each job to determine if the candidate possesses the skills needed to perform that job.

Candidates are selected, based on non-discriminatory practices, relevant work experience, skill level, and acceptable testing scores. Once selected, candidates are passed along for pre-screening interviews with HR and potentially the hiring manager.

The pre-screening process begins with an interview by HR and applies to both Neubus employees and to new hire candidates. This is a detailed interview with an overview of the company; the position that is being filled; the candidates work experience; behavioral interview questions; and reviewing the candidate's educational background. This interview provides HR with relevant information needed to match qualified candidates with the open positions and allows HR to pass or reject the candidate. This interview will be abbreviated for Neubus employees.

From these initial screening interviews, HR will move top candidates to the next steps in the process, which includes hiring manager interviews and background checks. Managers use a structured interview and evaluation guide in interviewing the candidates. This interview guide includes behavioral interview questions regarding the candidates past work experience, education, and other relevant work experiences. All interviewing managers are trained on correct interview practices.

In coordination with HR, the manager's top candidates progress to background checks. These checks provide nondiscriminatory information for the managers to use in candidate selection. Background checks for education, employment, references, and criminal history are an important indicator of the candidate's ability to perform as expected. Depending on the position, candidates, who may have access to company financial information for example, may also have credit background checks performed.

Any candidate, whether a Neubus employee or a new hire, will be prescreened to ensure that they are able to read, write, speak, and understand the English language.

Note: If an employee does not pass the background check(s) or does not meet the DIR customer's standards, he/she will immediately be withdrawn from consideration from working on the project or removed from the project if he/she has already started working on the project order.

All persons working at Neubus facilities must have submitted fingerprint-based criminal history checks and paperwork and have received clearance from the Texas Department of Public Safety (DPS). Additional DIR customer-specific criminal background checks are performed as needed and bonding (if required in the DIR Customer's project order) for personnel assigned to specific Customer projects (e.g. compliance with the FBI CJIS security addendum).

Upon hire, employees receive new hire orientation that incorporates our company culture and work/professional conduct expectations. The orientation session includes detailed training on Neubus company policies, security policies, and production/functional training. Neubus also conducts HIPAA, Diversity, and Harassment training at this time. Neubus' harassment training covers sex, race, age, religion, national origin, disability, and sexual orientation. Documentation of training completion will be made available to the DIR customer upon request.