SECOND AMENDATORY AGREEMENT

THIS SECOND AMENDATORY AGREEMENT is entered into as of the date indicated on the signature page, by and between the **CITY AND COUNTY OF DENVER**, a Colorado municipal corporation ("City"), Party of the First Part, and **OSP US INC.**, a corporation authorized to conduct business in the State of Colorado (the "Contractor"), Party of the Second Part;

WITNESSETH

WHEREAS, City and ACS Transport Solutions, Inc. entered into an Agreement dated October 1, 2013 which was subsequently amended on October 4, 2018, in which ACS Transport Solutions, Inc. agreed to provide professional and technical support services for the maintenance and operation of the Parking and Ground Transportation Revenue Control System ("PGTRCS") in order to assure the satisfactory operation of the City and County of Denver Department of Aviation's parking and ground transportation facilities operations; and

WHEREAS, said Agreement was subsequently assigned to Contractor by a Consent, Assignment and Novation Agreement executed by the parties on June 22, 2018; and

WHEREAS, said Agreement was then amended by a First Amendatory Agreement executed by the parties on October 4, 2018; and

WHEREAS, the parties desire to further amend the Agreement as set forth herein; and

NOW, THEREFORE, for and in consideration of the premises and other good and valuable consideration, the parties hereto agree as follows:

1. **Section 3.01 TERM** is hereby amended by deleting Section 3.01 in its entirety and replacing it with the following:

"**3.01 TERM**

The term of this Contract shall commence at 12:01 a.m. MST on October 1, 2013 and shall terminate at 12:00 a.m. MST on September 30, 2020, unless earlier terminated in accordance with the Contract Documents. At the expiration of the Term, as set forth in this Paragraph 3, the parties may mutually agree to extend the Term on a month-to-month basis by the City providing written notice to Contractor on or before September 1, 2020, which notice may be accepted by counter execution by Contractor within fifteen (15) days of receipt. Upon such acceptance, this Agreement shall continue in full force and effect on a month-to-month basis unless thirty (30) days written notice of termination is given by either party. However, no extension of the Contract Term shall increase the City's Maximum Contract Liability stated herein; such amount may be changed only by a duly executed written amendment to this Contract."

2. **Section 4.04 MAXIMUM LIABILITY** is hereby amended by deleting Section 4.04 in its entirety and replacing it with the following:

"**4.04 MAXIMUM LIABILITY**

Any other provision in this Contract notwithstanding, in no event shall the City be liable for payment under this Contract for any amount in excess of Twelve Million Five Hundred Thirty-Five Thousand Two Hundred Forty-Five Dollars and Zero Cents ($12,535,245.00). The Maximum Contract Liability may only be increased by amendment to this Contract. All payments under this Contract shall be paid solely and exclusively from the City and County of Denver, Funds of the Airport System and from no other fund or source. The City is under no obligation to make any future apportionments or allocations to said fund."

3. **Section 6.02 INDEMNIFICATION** is hereby amended by deleting Section 6.02 in its entirety and replacing it with the following:

"6.02 INDEMNIFICATION

The City cannot and by this Contract does not agree to indemnify, hold harmless, exonerate or assume the defense of the Contractor or any other person or entity whatsoever, for any purpose whatsoever.

The Contractor hereby agrees to defend, indemnify and hold harmless the City, its officers, agents and employees from and against any and all loss of or damage to property or injuries to or death of any person or persons, including property and employees or agents of the City, and shall defend, indemnify and hold harmless the City and its officers, agents and employees from any and all claims, damages, suits, costs, expenses, liability, actions or proceedings of any kind or nature whatsoever, of or by anyone whomsoever, including Workers' Compensation claims, in any way resulting from or arising out of, directly or indirectly, the Contractor's negligent or wrongful acts in connection with, or breach of this Contract or the work that is the subject of this Contract, or the Contractor's negligent or wrongful acts in the use or occupancy of City owned property or other property upon which work is performed under this Contract, including negligent and wrongful acts and omissions of the Contractor's officers, employees, representatives, suppliers, invitees, contractors and agents; provided, however, that the Contractor's obligation to indemnify and hold harmless the City, its officers, agents and employees under this paragraph shall not apply to liability or damages resulting from the sole negligence of the City's officers, agents and employees.

LIMITATION OF LIABILITY: Regardless of the basis on which the City is entitled to claim damages from Contractor (including, without limitation, breach of contract, negligence, misrepresentation, or other contract or tort claim), Contractor's entire liability for all claims in the aggregate arising from or related to services provided by this Agreement will not exceed $12 million dollars.

In addition to all other defense and indemnity obligations undertaken by the Contractor under this Contract, the Contractor and its subcontractors, to the extent that its performance of this Contract includes the allowance of utilization by members of the public of credit cards to pay monetary obligations to the City or the Contractor, or includes the utilization, processing, transmittal and/or storage of credit card data by the Contractor, shall defend, release, indemnify and save and hold harmless the City against any and all fines, penalties, assessments, costs, damages or other financial obligations, however denominated, assessed against the City and/or the Contractor and its subcontractors by credit card company(s), financial institution(s) or by the National Automated Clearing House Association (NACHA) or successor or related entity, including but not limited to,

any credit card company fines, regardless of whether considered to be consequential, special, incidental or punitive damages, costs of notifying parties and persons affected by credit card information disclosure, the cost of replacing active credit cards, and any losses associated with fraudulent transaction(s} occurring after a security breach with respect to credit card information, and shall defend, release, indemnify, and save and hold harmless the City from any and all claims, demands, suits, actions, liabilities, causes of action or legal or equitable proceedings of any kind or nature, of or by anyone whomsoever, in any way affected by such credit card data or utilizing a credit card in the performance by Contractor of this Contract. In furtherance of this Contractor covenant to defend and indemnify, the Contractor and its subcontractors shall perform the roles and responsibilities allocated to Contractor in Exhibit F to allow the City to maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS), based on the roles and responsibilities defined in Exhibit F, and with all other requirements and obligations related to credit card data or utilization set out in Exhibit A. Notwithstanding anything to the contrary in this section or elsewhere in this Agreement, Contractor shall be obligated to indemnify or defend the City against fines, penalties, assessments, costs, damages, claims, demands, suits, actions, liabilities, causes of action or legal or equitable proceedings related to credit card data or utilization, solely to the extent that such fines, penalties, assessments, costs, damages, claims, demands, suits, actions, liabilities, causes of action or legal or equitable proceedings are caused by Contractor's failure to perform a responsibility for which Contractor is responsible pursuant to Exhibit F, or its failure to perform a requirement or obligation set out in Exhibit A."

4. The following Section is added to the agreement- "**11.24 PAYMENT OF CITY MINIMUM WAGE**:

Contractor shall comply with, and agrees to be bound by, all requirements, conditions, and City determinations regarding the City's Minimum Wage Ordinance, Sections 20-82 through 20-84 D.R.M.C., including, but not limited to, the requirement that every covered worker shall be paid no less than the City Minimum Wage in accordance with the foregoing D.R.M.C. Sections. By executing this Agreement, Contractor expressly acknowledges that they are aware of the requirements of the City's Minimum Wage Ordinance and that any failure by Contractor or any other individual or entity acting subject to this Agreement, to strictly comply with the foregoing D.R.M.C. Sections shall result in the penalties and other remedies authorized therein."

5. **Exhibit A Scope of Work Section 12** is amended by deleting Section 12 in its entirety and replacing it with the following-

"12. <u>PCI Compliance</u>: This agreement requires OSP US, INC to provide verification to DEN, prior to start-up and on-going annually. During the term of this agreement, all modules of Contractor's system(s) that interface with, or utilize credit card information in any manner or form of collection, must be compliant with Payment Card Industry Data Security Standards ("PCI DSS) (provided that Contractor's sole responsibility for PCI DSS compliance shall be the responsibilities identified as Contractor's responsibilities in Exhibit F) and to include the Payment Application Data Security Standard ("PA DSS") certification of all systems or solutions utilized to provide payment processing services to DEN.

A. Contractor shall, verify PCI DSS compliance (based on the roles and responsibilities

defined in Exhibit F), and allow DEN's contracted PCI DSS compliance auditor full access to Contractor's system(s) installed at DEN at any time to provide this verification to DEN. If any association requires an audit of Contractor or any of Contractor's service providers, agents, business partners, contractors or subcontractors due to a data security compromise event, Contractor agrees to cooperate with such audit. DEN agrees to assist Contractor in obtaining a confidentiality agreement with any such auditor.

B. Contractor shall not retain or store CW2/CVC2 data subsequent to authorization of a credit card transaction. Contractor shall prohibit disclosure of any and all cardholder information, and in the event of a compromise of credit card information resulting from a PRCS application failure, or Contractor on-site maintenance personnel disclosure, Contractor shall immediately notify DEN in writing, and upon Contractor agreement, shall support appropriate notification to parties and persons affected by such disclosure and compromise.

C. Contractor agrees to comply with all applicable sections and subsections of the PCI DSS (provided that Contractor's sole responsibility for PCI DSS compliance shall be the responsibilities identified as Contractor's responsibilities in Exhibit F), as well as PA DSS, and (where applicable) the VISA Payment Application Best Practices (PABP)."

6. **Exhibit A Scope of Work Table 1** is hereby deleted and replaced with the attached **Table 1.**

7. **Exhibit B Standard Operating Procedures Section 4** is hereby deleted and replaced with the following-

"**Section 4 - PCI COMPLIANCE**

A. The contractor acknowledges that this contract requires the contractor to be responsible for administrative, technical and physical security of all sensitive data within their control. Sensitive data includes but is not limited to passwords, credit card information, and financial information. All contractor employees will receive security training during their new hire training period and at a minimum refresher training will occur annually. All security training will be documented and signed by the trainer and the trainee. At a minimum the security training documentation will list each item and the date of the training.

B. The contractor will protect all cardholder data as specified by the PCI DSS and in accordance with DIA standards, policies and procedures.

C. The contractor will report any known or suspected compromise of any data to the Contract Administrator immediately upon knowledge of the compromise or suspected compromise.

D. The contractor acknowledges that the company has ownership of cardholder data. The contractor also acknowledges that such data can only be used for assisting VISA or the acquiring bank in completing a transaction, supporting a loyalty

program, providing fraud control services, or such uses specifically required by law.

E. The contractor will allow access by VISA or VISA approved entities in the event of a cardholder data compromise.

F. The contractor will provide business continuity such that the services provided by the vendor will be available in the event of a major disruption of failure.

G. The contractor will ensure continued security of cardholder data during the life of the contract. The contractor shall ensure continued security of cardholder data after the termination of the contract until such time as the contractor no longer has card holder data in their possession and no longer has access to card holder data.

The contractor will allow access by any PCI OSS auditors as approved by the contract administrator. The City agrees to assist ACS in obtaining a confidentiality agreement with any such auditor.

H. The parties understand and agree that Contractor no longer offers the PRCS system to customers for new installation, and that it only maintains PA DSS certification for the PRCS system as an existing installation. Accordingly, and notwithstanding anything in the Agreement to the contrary, the parties agree that any material upgrades or updates to new or existing operating systems, databases, or PRCS applications, or other upgrades or updates to the PRCS system that are requested by Client during the remaining term of the Agreement or required after the date of this Amendment to allow for ongoing PA DSS or PCI DSS certification of the PRCS system will only be undertaken by Contractor at additional cost to the City, save that Contractor will continue to deploy maintenance related antivirus and operating system updates to existing systems that originate from their respective manufacturers. The rates charged by Contractor for such upgrade or updates will be negotiated in good faith and agreed between the parties before work on such upgrade or update commences."

8. **Exhibit F PRCS Roles and Responsibilities** is hereby attached and added to the Agreement.

9. All references in the Existing Agreement to "Conduent Transport Solutions Inc." are hereby deleted and replaced with "OSP US Inc." as the context may require.

10. This Second Amendatory Agreement shall not be effective or binding on the City until fully executed by all signatories of the City and County of Denver.

[END OF PAGE]

Contract Control Number: PLANE-201951328-02/Alfresco 201309652-02
Contractor Name: OSP US INC

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of:

SEAL

CITY AND COUNTY OF DENVER:

ATTEST:

By: _____

_____

APPROVED AS TO FORM:

Attorney for the City and County of Denver

By: _____

REGISTERED AND COUNTERSIGNED:

By: _____

By: _____

Contract Control Number: PLANE-201951328-02/Alfresco 201309652-02
Contractor Name: OSP US INC

By: DocuSigned by: Michael H. Bigbee 8730DA897D6D4B3...

Name: Michael H. Bigbee
(please print)

Title: CEO
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

TABLE 1 - SLA NON-PERFORMANCE OR SUBSTANDARD PERFORMANCE		
Service Level Agreement Criteria	**Measurement**	**Deductions**
Contractor shall maintain not less than the agreed number of properly trained and certified staff for Onsite Support Services as scheduled.	Contractor shall provide a monthly report showing on-site staff levels during the month.	Two (2) times the normal fee for the absent resource if the remaining staff does not provide coverage for the missing staff member.
Contractor shall ensure equipment is available ninety-nine percent (99%) of the scheduled uptime as approved by DEN.	Contractor shall provide a monthly report showing the actual uptime of each lane.	$200.00 per every percent below ninety-nine percent (99%) each device is down. Ticket jams and receipt paper jams do not count against availability.
Preventative maintenance shall be performed as scheduled pursuant to manufacturer's recommendations and as approved by DEN.	Contractor shall provide a monthly report showing the scheduled and completed activities for the previous month.	One percent (1%) of the total monthly fee for every percentage point below ninety percent (90%) of goal achievement.
Corrections to existing application software shall be completed within ninety (90) days of time of report. and after the fifteen (15) days validation period.	Contractor shall provide a release date for corrections to existing software. Such data will be considered in calendar days against the needed correction/defect accepted by Contractor and Contractor will have fifteen (15) days to validate software corrections and if they that are needed.	$50.00 each late day the activity is incomplete.
Contractor shall ensure ongoing PRCS compliance with applicable PA DSS requirements promulgated by the PCI-SSC, and shall ensure Contractor staff follows PCI-DSS related SOPs and the requirements of Exhibit F (but, in the case of PCI-DSS SOPs, solely to the extent that such SOP is identified as a Contractor responsibility in Exhibit F).	Contractor shall certify semi-annually that applicable PRCS application software is compliant with PA- DSS requirements. This certification is provided by an external PA-DSS auditor on an annual basis and can be resubmitted for the semi-annual certification to DEN.	$5,000.00 per certification incident ($10,000.00 per year maximum) plus $2000.00 per month if after 30 days Contractor fails to provide a remediation plan acceptable to the Airport Authority's financial institution. $5,000.00 per incident ($10,000.00 per maximum) for each incident where On-Site staff fails to follow PCl DSS related SOPs and Exhibit F.
Contractor shall provide all monthly Service Level Agreement reports within ten (10) calendar days following the end of each month.	DEN will determine the number of days each report is late.	$100.00 per each late day.

Exhibit F

Phase I Responses

Control No.	Request	Client Response	Responsible Party
RFI1.1	Business Description: Non-marketing explanation of the in-scope lines of business (retail, ecommerce, brick-n-mortar, etc.), operating locations, transaction volume, number of employees, number of IT employees, major IT contract providers.	Denver International Airport (DEN) Parking System provides parking facilities for patrons of Denver International Airport. Orbility (OSP) manages the technical processing environment for DEN Parking servers, workstations, and applications. Standard Parking provides DEN Parking with operating services to collect payment, attend the parking lanes and sales audit services. Denver International Airport Business Technologies (BT) provides the network infrastructure for routing and segmenting the cardholder environment from the rest of the business systems and operations. DEN Parking Management (DPM) is monitored and managed by The Commercial Division, Parking and Transportation section, under the Department of Aviation, City and County of Denver. For the management of the daily operations and revenue collections, the process is outsourced, through Contract, to Standard Parking +, under the management of CCD DEN Parking and Transportation. For the management of the DEN parking system cardholder payment systems has been outsourced, through Contract, to OSP. The outsource service provider has implement card processing as a part of its Parking Revenue Control System (PRCS) environment that is used at multiple airports throughout the country. The PRCS merchant ID has been specifically segmented from all other merchant processing to enable detailed sales audit and post processing verification. Parking services for the Orbility (OSP) environment include Pikes Peak, East/West Garages, East/West Valet, Short-term, East/West Economy parking lots, and the Mt. Elbert overflow lot. There are a total of 52 exit lanes in the parking lots where payment is taken and 7 entry lanes where credit cards may be used for "card-in" access. There are 120 employees and 13 IT employees that access the PRCS environment. Credit cards are also accepted for employee parking utilizing swipe machines that are supported by Chase Paymentech. For the purposes of this PCI DSS assessment, Denver International Airport (DEN) Parking System is considered a Level 2 merchant because they process between one and six million transactions.	DEN Parking & Transportation
RFI1.2	Client Scope Identification Process: Formal document detailing the organization's methodology and all of the processes used to identify and document all instances of cardholder data (electronic / paper), to include any data discovery tools or automated processes to ensure that no cardholder data exists outside of the in-scope environment. To be clear, this is not a definition of the organizations actual scope, but rather the continuous processes to ensure the scope is documented accurately at all times.	During annual risk assessment and ROC activities DEN goes through a scoping process that encompasses locating, verifying, and then documenting the cardholder data environment (CDE), to include all system components, people, and processes. The CDE is organized and analyzed to determine intended and authorized use, risk, and component connectivity. To help monitor potential cardholder activities outside the CDE, DEN uses a Data Loss Prevention (DLP) strategy to scan networks, SharePoint files and email files. DLP Tools are used to monitor data at rest and in motion and reports are checked periodically as part of DIA's Security Operations Center (SOC) Guide. Each potential credit card activity is opened, reviewed, recorded and if needed escalated as part of Incident Tracking process.	DEN Parking & Transportation, Orbility (OSP), Business Technologies
RFI1.3	Client Scope Narrative of the Cardholder Data Environment (CDE): Please provide a narrative of all the ways your organization accepts, transmits, stores or processes payment card transactions from data capture through settlement. (This narrative is the result of, and should be consistent with, the methodology explained in RFI1.2)	DEN accepts card-present credit card transactions for parking services. Cardholder data is taken by both manned and self-service kiosks from DEN parking customers as they exit the parking facilities. Cardholder data is transmitted to Chase Paymentech via a private circuit for authorization and settlement. o Within the CDE, cardholder data received from the POS swipe terminal is encrypted by the cashier terminal application at the exit lanes and valet stand prior to transmission over the internal network to the communication server, which communicates with Chase Payment tech for authorization. To prevent persistence of cardholder data, the cashier terminal application then sends a reset command to the POS swipe terminal to clear the terminal's buffer of any credit card information. o Cardholder transactions are processed using PA-DSS certified PRCS (in accordance with the applications deployment guidelines). o External transmission to Chase Paymentech for processing over private leased lines. o Only the last four digits of cardholder data may be accessed by a limited number of DEN sales audit staff through Chase Paymentech's SSL-secured website. Payment Processing: As a Level II merchant, Denver International Airport (DEN) Parking System accepts the following types of credit card transactions: DEN accepts card-present transactions conducted by a parking attendant and at self-serve (unstaffed) entries and exits. At self-serve (unstaffed) entries, the patron has the option to insert the card in lieu of taking a ticket. Card information (PAN) is transmitted to the Communication Server (CS), which transmits it to the Real Time Server and pairs it with a transaction number for processing when the patron exits. The parking attendant swipes the credit card though a card reader or manually types the card number if unreadable into the terminal attached to the cashier terminal. At self-serve exits, the customer inserts their credit card into a card reader. Card information (SAD and PAN) is transmitted to the Communication Server (CS), which transmits it to the Real Time Server (RTS) and then to Paymentech over a private point to point connection. As a part of transaction processing, sensitive authentication data is never stored and is only processed in the system's volatile memory. Card-Not-Present Transactions: DEN Parking does not accept or process card-not-present transactions. PIN/Debit Transactions: DIA Parking does not accept PIN/debit card transactions.	DEN Parking & Transportation, Orbility (OSP), SP+
RFI1.4	Supporting Diagram(s): All diagrams supporting the Client Scope Narrative The narrative needs to be accompanied by data flow diagram(s) that illustrate the flow of Cardholder Data (CHD) into, throughout and out of the Cardholder Data Environment (CDE). Details on the diagram requirements are included in the sub-sections below. High-level Network Diagram(s) – Executive Summary Section 2.2 Detailed Network Diagram(s) – Executive Summary Section 4.1 Dataflow Diagram(s) – Executive Summary Section 4.2 Note: There is a disconnect between the level of detail requested in the reporting template and the title of the diagram for executive summary 2.2 and executive summary 4.1. The High-level Network Diagram requests a significant amount of granular detail while the Detailed Network Diagram is more of an overview with less granularity. This is backwards from what their title would suggest. The narrative needs to be accompanied by data flow diagram(s) that illustrate the flow of Cardholder Data (CHD) into, throughout and out of the Cardholder Data Environment (CDE). Details on the diagram requirements are included in the sub-sections below.	See below for each section	DEN Parking & Transportation
RFI1.4a	High-level Network Diagram(s) 1. All physical locations in the report need to be represented clearly on the diagram(s) 2. Diagram(s) needs to clearly show in-scope and out-of-scope segments. This is best achieved with shaded boxes around each area with a key to explain colors/shading. 3. All inbound and outbound connections to the CDE must be represented in the diagram(s). Communication outside the CDE needs to show protections for card data inbound/outbound. 4. Inside the CDE, segmentation should be clearly illustrated. For large, complex environments, representative segmentation can be used. 5. All segments need to be clearly labeled, labels must match any segmentation narratives provided. 6. Wireless segments should be specifically called out in the diagram with appropriate icons. 7. All devices providing segmentation must be clearly labeled on the diagram(s). 8. Representative icons on the diagrams must exist for all security devices related to controls, any system in the payment flow, and other any other critical / key systems providing services to the CDE. 9. Diagram should be dated, including a "reviewed by" date that is within the current assessment year. 10. Virtualization technologies should be clearly identified on the diagram separately indicating the hypervisor, related management hosts, and then the actual virtual/guest systems. 11. A key to explain the diagram icons and coloring/shading.	see Phase 1 Drawing Narratives tab for current list and versions	Orbility (OSP), Business Technologies

RFI1.4b	Detailed Network Diagram(s) Note: This diagram aligns most with PCI Requirement 1.1.2 1. Clearly illustrates CDE versus non-CDE 2. Clearly illustrates all connections to the CDE from areas outside the CDE. 3. Clearly illustrates all known wireless devices both in and out of the CDE. 4. Clearly illustrates all connections to third-parties, card brands, or other business units. 5. Clearly illustrates all physical locations in the report on compliance. 6. For connections inbound/outbound of the CDE any protections on the transmitted card data must be included. 7. All included segments must be labeled. Labels used need to be the same across all diagrams in the entire report for reconciliation purposes. 8. A key to explain the diagram icons and coloring/shading. 9. Diagram should be dated, including a "reviewed by" date that is within the current assessment year.	see Phase 1 Drawing Narratives tab for current list and versions	Orbility (OSP)
RFI1.4c	Dataflow Diagram(s) Note: This diagram aligns with PCI Requirement 1.1.3 1. Diagram(s) are intended to work in conjunction with 4.2 dataflow narratives to provide a holistic view of the in scope environment, illustrating inbound, internal, and outbound flows. 2. Diagram(s) should visually depict any and all storage, processing, or transmission of cardholder data. 3. Diagram(s) are expected to be unique and not the network diagram re-used with lines drawn on it. 4. Diagram(s) must align with the network diagram with respect to locations, CDE boundaries, devices, and data protections. If the diagram includes information on the network diagrams, use the same labels. 5. Diagram(s) should be dated, including a "reviewed by" date that is within the current assessment year. 6. Cover all acceptance channels/processing flows of cardholder data provided in the report for card present, card-not-present, PIN/Debit: • Capture, Authorization, Settlement, Chargeback • Any other flows of any card data as applicable to the assessed environment • Additionally for a managed service provider with no card data, cover any process that is covered in the assessment 7. For each step of the flow, show all payment applications. 8. For each step of the flow, show any and all storage and protections applied to the stored data. 9. For communication across open / public networks or untrusted networks, indicate the protections on the communication channel. 10. Wireless segments/transmission in the dataflow should be indicated in the diagram(s).	see Phase 1 Drawing Narratives tab for current list and versions	DEN Parking & Transportation, Orbility (OSP)
RFI1.5	CDE Inventory: Please fully complete the CDE Inventory spreadsheet (Located on the project portal under Client Provided Documents>EDC). The inventory should be consistent with all of the information provided above. NOTE: The content of the CDE Inventory spreadsheet is vital, the format is not. If your organization maintains this information in another format that contains (at a minimum) all of the information included in the CDE Inventory spreadsheet, feel free to submit that instead. A Completed CDE Inventory is critical for scheduling and sampling purposes.	See DEN PCI Inventory	DEN Parking & Transportation, Orbility (OSP), Business Technologies, SP+
RFI1.POC	Point of Contact: Provide the contact information for the Company Point of Contact for this assessment.	Tim Coogan –DIA Technologies CISO 8500 Pena Blvd, Denver, CO 80249-6340 Phone: (303) 342-4741 Email: tim.coogan@flydenver.com	Business Technologies
RFI1.AOC	Client Officer: Provide the name of the company Officer that will be signing the final Attestation of Compliance (AOC) for this project.	Tim Coogan –DIA Technologies CISO 8500 Pena Blvd, Denver, CO 80249-6340 Phone: (303) 342-4741 Email: tim.coogan@flydenver.com	Business Technologies

Exhibit F
Phase I Drawing Narratives

Drawing Name	RFI Response Level	Responsible Party	Narrative	Current Version name
PRCS SAN Master Topology	Detailed	Orbility (OSP)	Full overview Diagram of PRCS Networks	O19 8_2 PRCS Master_Topology_REV3.2
Conduent Parking Revenue and Control System	Detailed	Orbility (OSP)	Process Chart of the PRCS Card Holder data flow proces	O19 8_14 Parking Revenue Control System 8x - Card Holder Data Flow Rev 4_1
WebPRCS_System Communication Flows	Data Flow	Orbility (OSP)	Process Chart for WebPRCS communication	O19 1_1_6 Conduent WebPRCS System Communication Flows 2018
PRCS Card Holder Data Flow	Data Flow	Orbility (OSP)	Process for Credit Data Flow	O19 8_14 Parking Revenue Control System 8x - Cardholder Data Flow Rev 4_1
PRCS Test Network Topology	Detailed	Orbility (OSP)	Diagram of the PRCS Test Network	O19 8_2 PRCS Test Network Topology_rev 1.0
PRCS Master Topology	Detailed	Orbility (OSP)	Diagram of the PRCS Production Network	O19 8_2 PRCS Master_Topology_REV3.2
PRCS High Level Topology	High Level	Orbility (OSP)	High Level Overview Diagram of PRCS Network	O19 8_2 PRCS High Level Topology_rev 1.2
PRCS Server System Overview Architect	Detailed	Orbility (OSP)	Overview Diagram of PRCS Servers	O19 8_2 PRCS Server System Overview Architecht_rev3.0
PRCS Reference Baseline Topology (Definitions	Supplement	Orbility (OSP)	PRCS System Reverence Manual	O19 7_1 PRCS Reference Baseline Topology v1
PPSO Credit Card processing	Process Flow	DEN Parking & Transportation	Processes for Credit Card Purchases within the Parking I	P18 1_1_3 PPSO CC Processing
GT CC processing flow chart	Process Flow	DEN Parking & Transportation	Diagram for processing for Credit Card Purchases at the	P18 1_1_3 GT CC processing flow chart
Parking Mgmt Data Process	Process Flow	DEN Parking & Transportation	Securing Credit Card Data	P18 3_1 Data Retention
PRCS_Network_DIAGRAM	High Level	Business Technologies	See Narratives Tab in document	T19 1_1 PRCS Network Reviewed 180306 v2

Exhibit F
3.2 Requirements

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
	1: Install and maintain a firewall configuration to protect cardholder data				
1.1	Establish and implement firewall and router configuration standards that include the following:				
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	***1.1.1*** *A formal process for approving and testing all network connections and changes to the firewall and router configurations. Examine documented procedures to verify there is a formal process for testing and approval of all:* *• Network connections, and* *• Changes to firewall and router configurations.*	Procedure	Change Management	Business Technologies
1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	***1.1.2*** *Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.* *Identify the document examined to verify processes require that the network diagram is kept current.*	Policy	Information Security	Business Technologies Business Technologies
1.1.3	Current diagram that shows all cardholder data flows across systems and networks		Diagrams		Orbility (OSP) Business Technologies DEN Parking & Transportation
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	***1.1.4*** *Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.* *Identify the firewall configuration standards document examined to verify requirements for a firewall:* *• At each Internet connection.* *• Between any DMZ and the internal network zone.*	Configuration Standard	Firewall Configuration Standard	Business Technologies
1.1.5	Description of groups, roles, and responsibilities for management of network components	***1.1.5*** *Description of groups, roles, and responsibilities for management of network components.* *Identify the firewall and router configuration standards document(s) reviewed to verify they include a description of groups, roles and responsibilities for management of network components.*	Configuration Standard	Firewall Configuration Standard Router Configuration Standard	Business Technologies Business Technologies
1.1.6	Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	***1.1.6*** *Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.* *Identify the configuration standards document(s) reviewed to verify the document(s) contains a list of all services, protocols and ports necessary for business, including a business justification for each.*	Configuration Standard	Firewall Configuration Standard Router Configuration Standard	Orbility (OSP) Orbility (OSP)
1.1.7	Requirement to review firewall and router rule sets at least every six months	***1.1.7*** *Requirement to review firewall and router rule sets at least every six months.* *Identify the firewall and router configuration standards reviewed to verify they require a review of firewall rule sets at least every six months.*	Configuration Standard	Firewall Configuration Standard Router Configuration Standard	Business Technologies Business Technologies
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	***1.2.1*** *Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.* *Identify the firewall and router configuration standards reviewed to verify they identify inbound and outbound traffic necessary for the cardholder data environment.*	Configuration Standard	Firewall Configuration Standard Router Configuration Standard	Business Technologies
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.				
1.2.2	Secure and synchronize router configuration files.				

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.				
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	***1.3.8*** *Do not disclose private IP addresses and routing information to unauthorized parties.* *Identify the document reviewed that specifies whether any disclosure of private IP addresses and routing information to external parties is permitted.*	Policy	Network Policy	Business Technologies
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.				
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.				
1.3.3	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)				
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.				
1.3.5	Permit only "established" connections into the network.				
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.				
1.3.7	Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: • Network Address Translation (NAT) • Placing servers containing cardholder data behind proxy servers/firewalls, • Removal or filtering of route advertisements for private networks that employ registered addressing, • Internal use of RFC1918 address space instead of registered addresses.				
1.4	Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	***1.4*** *Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network.* *Examine policies and configuration standards to verify:* *• Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet (for example, laptops used by employees) when outside the network, and which are also used to access the network.* *• Specific configuration settings are defined for personal firewall software.* *• Personal firewall software is configured to actively run.* *• Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices.*	Policy	Employee Use	Orbility (OSP)

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	***1.5*** *Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.* *Identify the document reviewed to verify that security policies and operational procedures for managing firewalls are documented.*	Policy and Operational Procedures	Network Policy	Business Technologies
	2: Do not use vendor-supplied defaults for system passwords and other security parameters				
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a	*See all documents listed from marked 2.1 to 2.5*			Business Technologies Business Technologies Orbility (OSP)
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Wireless not allowed in CDE environment			
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	See all documents in 2.0			
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	See all documents in 2.0			
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	See all documents in 2.0			
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	See all documents in 2.0			
2.2.4	Configure system security parameters to prevent misuse.	See all documents in 2.0			
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	See all documents in 2.0			
2.3	Encrypt all non-console administrative access using strong cryptography. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	See all documents in 2.0			

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	See all documents in 2.0			
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	See all documents in 2.0			
2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.	See all documents in 2.0			
	3: Protect stored cardholder data				
3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	***3.1*** *Keep cardholder data storage to a minimum by implementing data-retention and disposal policies, procedures and processes that include at least the following for all CHD storage:* *• Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements.* *• Processes for secure deletion of data when no longer needed.* *• Specific retention requirements for cardholder data.* *• A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.*	Policy and Operational Procedures	Data Handling, Retention and Disposal	Orbility (OSP) DEN Parking & Transportation
3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	*3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.* ***Identify*** *the documentation reviewed to verify there is a documented business justification for the storage of sensitive authentication data.* ***Identify*** *the document(s) reviewed to verify that it defines processes for securely deleting the data to verify that the data is unrecoverable.*	Policy and Operational Procedures	Data Handling, Retention and Disposal	Orbility (OSP)

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
3.2.1	Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained: • The cardholder's name • Primary account number (PAN) • Expiration date • Service code To minimize risk, store only these data elements as needed for business.				
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.				
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.				
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.	*3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.* ***Identify*** *the document(s) reviewed to verify that written policies and procedures for masking the displays of PANs include the following:* *• A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access.* *• PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN.* *• All other roles not specifically authorized to see the full PAN must only see masked PANs.*	Policy	Data Handling, Retention and Disposal	Orbility (OSP)
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	*3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:* *• One-way hashes based on strong cryptography, (hash must be of the entire PAN).* *• Truncation (hashing cannot be used to replace the truncated segment of PAN).* *• Index tokens and pads (pads must be securely stored).* *• Strong cryptography with associated key-management processes and procedures.* *Identify the documentation about the system used to protect the PAN examined.*	Policy	Encryption	Orbility (OSP)

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.				
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: Note: This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.	***3.5*** *Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.* *Identify the documented key-management policies and processes examined to verify processes are defined to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:* *• Access to keys is restricted to the fewest number of custodians necessary.* *• Key-encrypting keys are at least as strong as the data-encrypting keys they protect.* *• Key-encrypting keys are stored separately from data-encrypting keys.* *• Keys are stored securely in the fewest possible locations and forms.*	Policy and Operational Procedures	Encryption	Orbility (OSP)
3.5.1	Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and other SCDs used for key management Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.				
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.				
3.5.3	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method Note: It is not required that public keys be stored in one of these forms.	***3.5.2*** *Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times.* *Identify the documented procedures examined to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.* *• Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key.* *• Within a secure cryptographic device (such as a host security module (HSM) or PTS- approved point-of-interaction device).* *• As key components or key shares, in accordance with an industry-accepted method.*	Procedure	Encryption	Orbility (OSP)

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
3.5.4	Store cryptographic keys in the fewest possible locations.				
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.	***3.6*** *Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data:* ***Identify*** *the documented key-management procedures examined to verify procedures specify how to generate strong keys.* ***Identify*** *the documented key-management procedures examined to verify procedures specify how to securely distribute keys.* ***Identify*** *the documented key-management procedures examined to verify procedures specify how to securely store keys.* ***Identify*** *the document that defines:* *• Key crypto period(s) for each key type in use* *• A process for key changes at the end of the defined crypto period(s)* ***Identify*** *the key-management document examined to verify that key-management processes specify the following:* *• The retirement or replacement of keys when the integrity of the key has been weakened.* *• The replacement of known or suspected compromised keys.* *• Any keys retained after retiring or replacing are not used for encryption operations.* ***Identify*** *the document examined to verify that manual clear-text key-management procedures define processes for the use of the following:* *• Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND* *• Dual control of keys, such that at least two people are required to perform any key- management operations and no one person has access to the authentication materials of another.* ***Identify*** *the document examined to verify that key-management procedures specify processes to prevent unauthorized substitution of keys.* ***Identify*** *the document examined to verify that key-management procedures specify processes for key custodians to acknowledge that they understand and accept their key- custodian responsibilities.*	Procedure	Encryption	Orbility (OSP)
3.6.1	Generation of strong cryptographic keys				
3.6.2	Secure cryptographic key distribution				
3.6.3	Secure cryptographic key storage				
3.6.4	Cryptographic key changes for keys that have reached the end of their crypto period (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).				
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.				
3.6.6	If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. Note: Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.				
3.6.7	Prevention of unauthorized substitution of cryptographic keys.				
3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.				
3.7	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	***3.7*** *Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.* *Identify the document reviewed to verify that security policies and operational procedures for protecting stored cardholder data are documented.*	Policy and Operational Procedures	Encryption	Orbility (OSP)

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
	4: Encrypt transmission of cardholder data across open, public networks				
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS). • Satellite communications.	***4.1*** *Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following:* *• Only trusted keys and certificates are accepted.* *• The protocol in use only supports secure versions or configurations.* *• The encryption strength is appropriate for the encryption methodology in use.* ***Identify*** *the documented standards examined.* ***Identify*** *the document reviewed to verify that processes are specified for the following:* *• For acceptance of only trusted keys and/or certificates.* *• For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported).* *• For implementation of proper encryption strength per the encryption methodology in use.*	Policy	Network Policy	Orbility (OSP)
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	Wireless not allowed in CDE environment			
4.2	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	*4.2 Never send unprotected PANs by end-user messaging technologies.* ***Identify*** *the policy document stating that unprotected PANs must not be sent via end- user messaging technologies.* ***Identify*** *the policy document that explicitly prohibits PAN from being sent via end-user messaging technologies under any circumstance.*	Policy	Employee Use	Orbility (OSP)
4.3	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	***4.3*** *Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.* *Identify the document reviewed to verify that security policies and operational procedures for encrypting transmissions of cardholder data are documented.*	Policy	Information Security	Orbility (OSP)
	5: Use and regularly update anti-virus software or programs				
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	***5.1.1*** *Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.* ***Identify*** *the vendor documentation reviewed to verify that anti-virus programs:* *• Detect all known types of malicious software,* *• Remove all known types of malicious software, and* *• Protect against all known types of malicious software.*	Vendor Documentation	Vendor Documentation	Business Technologies
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	See all documents in 5.1			
5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.				
5.2	Ensure that all anti-virus mechanisms are maintained as	***5.2*** *Ensure that all anti-virus mechanisms are maintained as*	Policy and Operational	Anti-Virus	Business Technologies

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
	follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	*follows:* *• Are kept current.* *• Perform periodic scans.* *• Generate audit logs which are retained per PCI DSS Requirement 10.7.* *Identify the documented policies and procedures examined to verify that anti-virus software and definitions are required to be kept up to date.*	Procedures		
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.	See all documents in 5.2			
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	See all documents in 5.2			
	6: Develop and maintain secure systems and applications				
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.	***6.1*** *Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.* *Identify the documented policies and procedures examined to confirm that processes are defined:* *• To identify new security vulnerabilities.* *• To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities.* *• To include using reputable outside sources for security vulnerability information.*	Policy and Operational Procedures	Vulnerability	Business Technologies
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	***6.2*** *Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.* *Identify the documented policies and procedures related to*	Policy and Operational Procedures	Patching	Orbility (OSP) Orbility (OSP) Business Technologies Business Technologies

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
	Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	*security-patch installation examined to verify processes are defined for:* *• Installation of applicable critical vendor- supplied security patches within one month of release.* *• Installation of all applicable vendor-supplied security patches within an appropriate time frame.*			Business Technologies
6.3	Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle Note: This applies to all software developed internally as well as bespoke or custom software developed by a third party.	*6.3 Develop internal and external software applications (including web-based administrative access to applications) securely.* ***Identify*** *the document that defines software development processes based on industry standards and/or best practices.* ***Identify*** *the documented software development processes examined to verify that information security is included throughout the life cycle.*	SDLC	SDLC	Orbility (OSP)
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	***6.3.1*** *Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.* *Identify the documented software-development processes examined to verify processes define that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.*	SDLC	SDLC	Orbility (OSP)
6.3.2	Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release. Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	***6.3.2*** *Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes)* *Identify the documented software-development processes examined to verify processes define that all custom application code changes must be reviewed (using either manual or automated processes) as follows:* *• Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices.* *• Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5).* *• Appropriate corrections are implemented prior to release.* *• Code-review results are reviewed and approved by management prior to release.*	SDLC	SDLC	Orbility (OSP)

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:	***6.4*** *Follow change control processes and procedures for all changes to system components.* *Identify the documented policies and procedures examined to verify that the following are defined:* *• Development/test environments are separate from production environments with access control in place to enforce separation.* *• A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.* *• Production data (live PANs) are not used for testing or development.* *• Test data and accounts are removed before a production system becomes active.* *• Change-control procedures related to implementing security patches and software modifications are documented.*	Policy and Operational Procedures	Change Management	Orbility (OSP)
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	See all documents in 6.4			
6.4.2	Separation of duties between development/test and production environments				
6.4.3	Production data (live PANs) are not used for testing or development				
6.4.4	Removal of test data and accounts from system components before the system becomes active/goes into production.				
6.4.5	Change control procedures must include the following:				
6.4.5.1	Documentation of impact.				
6.4.5.2	Documented change approval by authorized parties.				
6.4.5.3	Functionality testing to verify that the change does not adversely impact the security of the system.				
6.4.5.4	Back-out procedures.				
6.4.6	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.				
6.5	Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	***6.5*** *Address common coding vulnerabilities in software-development processes as follows:* *• Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.* *• Develop applications based on secure coding guidelines.* ***Identify*** *the document reviewed to verify that training in secure coding techniques is required for developers.* ***Identify*** *the software-development policies and procedures examined to verify that processes are in place to protect applications from, at a minimum, the vulnerabilities listed in requirements 6.5.1-6.5.10.*	SDLC	SDLC	Orbility (OSP)
	Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external).	See all documents in 6.5			
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.				
6.5.2	Buffer overflows				

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
6.5.3	Insecure cryptographic storage				
6.5.4	Insecure communications				
6.5.5	Improper error handling				
6.5.6	All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).				
Note:	Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):				
6.5.7	Cross-site scripting (XSS)				
6.5.8	Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).				
6.5.9	Cross-site request forgery (CSRF)				
6.5.10	Broken authentication and session management				
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	***6.6*** *For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks* *Identify the documented processes that were examined to verify that public-facing web applications are reviewed using the tools and/or methods indicated above, as follows:* *• At least annually.* *• After any changes.* *• By an organization that specializes in application security.* *• That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment.* *• That all vulnerabilities are corrected* *• That the application is re-evaluated after the corrections.*	Procedure	Vulnerability	Orbility (OSP)
6.7	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	***6.7*** *Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.* *Identify the document reviewed to verify that security policies and operational procedures for developing and maintaining secure systems and applications are documented.*	Policy and Operational Procedures	Information Security	Orbility (OSP)
	7: Restrict access to cardholder data by business need to know				
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	***7.1*** *Limit access to system components and cardholder data to only those individuals whose job requires such access.* *Identify the written policy for access control that was examined to verify the policy incorporates the follows:* *• Defining access needs and privilege assignments for each role.* *• Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities.* *• Assignment of access based on individual personnel's job classification and function* *• Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.*	Policy	Access Control	Orbility (OSP) Orbility (OSP) Business Technologies Business Technologies Business Technologies
7.1.1	Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	See all documents in 7.1			
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.				

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
7.1.3	Assign access based on individual personnel's job classification and function.				
7.1.4	Require documented approval by authorized parties specifying required privileges.				
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:	***7.2*** *Examine system settings and vendor documentation to verify that an access control system is implemented* *Identify vendor documentation examined to confirm that access control systems are in place on all system components.*	Vendor Documentation	Vendor Documentation	Orbility (OSP) Orbility (OSP) Business Technologies Business Technologies Business Technologies
7.2.1	Coverage of all system components	See all documents in 7.2			
7.2.2	Assignment of privileges to individuals based on job classification and function.				
7.2.3	Default "deny-all" setting.				
7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	***7.3*** *Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.* *Identify the document reviewed to verify that security policies and operational procedures for restricting access to cardholder data are documented.*	Policy and Operational Procedures	Access Control	Orbility (OSP) Orbility (OSP) Business Technologies Business Technologies Business Technologies
	8: Assign a unique ID to each person with computer access				
8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	***8.1*** *Define and implement policies and procedures to ensure proper user identification management for non- consumer users and administrators on all system components as follows:* *Identify the written procedures for user identification management examined to verify processes are defined for each of the items below at 8.1.1 through 8.1.8:* *• Assign all users a unique ID before allowing them to access system components or cardholder data.* *• Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.* *• Immediately revoke access for any terminated users.* *• Remove/disable inactive user accounts at least every 90 days.* *• Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:* *- Enabled only during the time period needed and disabled when not in use.* *- Monitored when in use.* *• Limit repeated access attempts by locking out the user ID after not more than six attempts.* *• Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.* *• If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*	Procedure	Access Control	Orbility (OSP) Orbility (OSP) Business Technologies Business Technologies Business Technologies
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	See all documents in 8.1			
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.				
8.1.3	Immediately revoke access for any terminated users.				
8.1.4	Remove/disable inactive user accounts within 90 days.				
8.1.5	Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.				
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.				
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.				

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.				
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	*8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.* *Identify the document examined to verify that authentication procedures for modifying authentication credentials define that if a user requests a reset of an authentication credential by a non-face-to-face method, the user's identity is verified before the authentication credential is modified.*	Procedure	Access Control	Orbility (OSP) Orbility (OSP) Business Technologies Business Technologies Business Technologies
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	See all documents in 8.2			
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.				
8.2.3	Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.				
8.2.4	Change user passwords/passphrases at least once every 90 days.				
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.				
8.2.6	Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.				
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	*8.2.3 SERVICE PROVIDERS ONLY* *Passwords/phrases must meet the following:* *Identify the documented internal processes and customer/user documentation reviewed to verify that*	Policy	Access Control	Orbility (OSP) Orbility (OSP) Business Technologies Business Technologies
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	See all documents in 8.3			
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.				
8.4	Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials	***8.4*** *Document and communicate authentication procedures and policies to all users.* *suspicion the password could be compromised.* ***Identify*** *the documented procedures examined to verify*	Procedure	Access Control	Orbility (OSP) Orbility (OSP) Business Technologies

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
	• Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	***Identify*** *the documented procedures examined to verify authentication procedures define that authentication procedures and policies are distributed to all users.* ***Identify*** *the documented authentication procedures and policies that are distributed to users reviewed to verify they include:* *• Guidance on selecting strong authentication credentials.* *• Guidance for how users should protect their authentication credentials.* *• Instructions for users not to reuse previously used passwords.* *• That users should change passwords if there is any suspicion the password could be compromised.*			Business Technologies
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	***8.5*** *Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:* *• Generic user IDs are disabled or removed.* *• Shared user IDs do not exist for system administration and other critical functions.* *• Shared and generic user IDs are not used to administer any system components.* ***Identify*** *the documented policies/procedures examined to verify authentication policies/procedures define that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited.*	Procedure	Access Control	Orbility (OSP) Orbility (OSP) Business Technologies Business Technologies Business Technologies Business Technologies
8.5.1	Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.	***8.5.1 SERVICE PROVIDERS ONLY*** ***Best practice until June 30, 2015*** *Additional requirement for service providers: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.* *Identify the documented procedures examined to verify that different authentication is used for access to each customer.*	Procedure	Access Control	Business Technologies
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	***8.6*** *Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned as follows:* *Identify the documented authentication policies and procedures examined to verify the procedures for using authentication mechanisms define that:* *• Authentication mechanisms are assigned to an individual account and not shared among multiple accounts.* *• Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.*	Policy and Operational Procedures	Access Control	Business Technologies
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).				Orbility (OSP)
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	***8.8*** *Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.* *Identify the document reviewed to verify that security policies and operational procedures for identification and authentication are documented.*	Policy and Operational Procedures	Access Control	Business Technologies Business Technologies
	9: Restrict physical access to cardholder data				

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.				Business Technologies
9.1.1	Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.				Business Technologies
9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.				Business Technologies
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	*Wireless not allowed in CDE environment*			
9.2	Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	***9.2*** *Develop procedures to easily distinguish between onsite personnel and visitors* ***Identify*** *the documented processes reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:* *• Identifying new onsite personnel or visitors (for example, assigning badges),* *• Changing access requirements, and* *• Revoking terminated onsite personnel and expired visitor identification (such as ID badges).* ***Identify*** *the document that defines that access to the identification process is limited to authorized personnel.*	Policy and Operational Procedures	Access Control	Orbility (OSP)
9.3	Control physical access for onsite personnel to sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.				Business Technologies
9.4	Implement procedures to identify and authorize visitors. Procedures should include the following:				Business Technologies
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.				Business Technologies
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.				Business Technologies
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.				Business Technologies

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.				Business Technologies
9.5	Physically secure all media.	***9.5 Physically secure all media.*** ***Identify the documented procedures for protecting cardholder data reviewed to verify controls for physically securing all media are defined.***	**Policy and Operational Procedures**	**Data Handling, Retention and Disposal**	Orbility (OSP) Business Technologies Business Technologies
9.5.1	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	***9.5.1*** *Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.* *Identify the document reviewed to verify that the storage location must be reviewed at least annually.*	Policy	Data Handling, Retention and Disposal	Business Technologies
9.6	Maintain strict control over the internal or external distribution of any kind of media, including the following:	***9.6*** *Maintain strict control over the internal or external distribution of any kind of media.* ***Identify*** *the documented policy to control distribution of media that was reviewed to verify the policy covers all distributed media, including that distributed to individuals.* ***Identify*** *the documented policy reviewed to verify policy defines how media is classified.*	Policy	Data Handling, Retention and Disposal	Business Technologies Orbility (OSP)
9.6.1	Classify media so the sensitivity of the data can be determined.				Business Technologies
9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.				Business Technologies
9.6.3	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).				Business Technologies
9.7	Maintain strict control over the storage and accessibility of media.	***9.7*** *Maintain strict control over the storage and accessibility of media.* *Identify the documented policy for controlling storage and maintenance of all media that was reviewed to verify that the policy defines required periodic media inventories.*	Policy	Data Handling, Retention and Disposal	Business Technologies Orbility (OSP) Orbility (OSP)
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.		Matrix	Inventory	Business Technologies
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:	***9.8*** *Destroy media when it is no longer needed for business or legal reasons* *Identify the policy document for periodic media destruction that was examined to verify it covers all media and defines requirements for the following:* *• Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard- copy materials cannot be reconstructed.* *• Storage containers used for materials that are to be destroyed must be secured.* *• Cardholder data on electronic media must be rendered unrecoverable via a secure wipe program (in accordance with industry- accepted standards for secure deletion), or by physically destroying the media.*	Policy	Data Handling, Retention and Disposal	Orbility (OSP) Business Technologies Orbility (OSP)
9.8.1	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.				Business Technologies
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.				Business Technologies

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. Note: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.	***9.9 Best practice until June 30, 2015*** *Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.* ***Identify*** *the documented policies and procedures examined to verify they include:* *• Maintaining a list of devices.* *• Periodically inspecting devices to look for tampering or substitution.* *• Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices.* ***Identify*** *the documented up-to-date list of devices examined to verify it includes:* *• Make, model of device.* *• Location of device (for example, the address of the site or facility where the device is located).* *• Device serial number or other method of unique identification.* ***Identify*** *the documented procedures examined to verify that processes are defined to include the following:* *• Procedures for inspecting devices.* *• Frequency of inspections.*	Policy and Operational Procedures	POI Security	Orbility (OSP)
9.9.1	Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.	See all documents in 9.9			
9.9.2	Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.				
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	***9.9.3 Best practice until June 30, 2015*** *Provide training for personnel to be aware of attempted tampering or replacement of devices.* *Identify the training materials for personnel at point-of-sale locations that were reviewed to verify the materials include training in the following:* *• Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.* *• Not to install, replace, or return devices without verification.* *• Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).* *• Reporting all suspicious behavior to appropriate personnel (for example, a manager or security officer).* *• Reporting tampering or substitution of devices.*	Policy	Training	Orbility (OSP) SP+
9.10	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	***9.10*** *Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.* *Identify the document reviewed to verify that security policies and operational procedures for restricting physical access to cardholder data are documented.*	Policy and Operational Procedures	Information Security	Orbility (OSP) Business Technologies
	10: Track and monitor all access to network resources and cardholder data				

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
10.1	Implement audit trails to link all access to system components to each individual user.				Orbility (OSP)
10.2	Implement automated audit trails for all system components to reconstruct the following events:				Orbility (OSP)
10.2.1	All individual user accesses to cardholder data				Orbility (OSP)
10.2.2	All actions taken by any individual with root or administrative privileges				Orbility (OSP)
10.2.3	Access to all audit trails				Orbility (OSP)
10.2.4	Invalid logical access attempts				Orbility (OSP)
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges				Orbility (OSP)
10.2.6	Initialization, stopping, or pausing of the audit logs				Orbility (OSP)
10.2.7	Creation and deletion of system-level objects				Orbility (OSP)
10.3	Record at least the following audit trail entries for all system components for each event:				Orbility (OSP)
10.3.1	User identification				Orbility (OSP)
10.3.2	Type of event				Orbility (OSP)
10.3.3	Date and time				Orbility (OSP)
10.3.4	Success or failure indication				Orbility (OSP)
10.3.5	Origination of event				Orbility (OSP)
10.3.6	Identity or name of affected data, system component, or resource.				Orbility (OSP)
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).	***10.4*** *Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.* ***Identify*** *the documented time-synchronization process that defines processes for ensuring the time synchronization technologies are kept current per PCI DSS Requirements 6.1 / 6.2.* ***Identify*** *the documented process for acquiring, distributing, and storing the correct time within the organization examined to verify that the process defines the following:* *• Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.* *• Where there is more than one designated time server, the time servers peer with one another to keep accurate time.* *• Systems receive time information only from designated central time server(s).* ***Identify*** *the documented time-synchronization procedures examined to verify procedures define that:* *• Access to time data is restricted to only personnel with a business need to access time data./• Define which personnel have a business need to access time data.* ***Identify*** *the documented time-synchronization procedures examined to verify procedures define that changes to time settings on critical systems must be:* *• Logged/• Monitored/• Reviewed* ***Identify*** *the document reviewed to verify it defines that:* *• Time settings are configured to either accept time updates from specific, industry-accepted time sources; OR* *• The updates are encrypted with a symmetric key and access control lists specify the IP addresses of client machines that will be provided with the time updates.*	Policy and Operational Procedures	Network Policy	Orbility (OSP) Orbility (OSP) Business Technologies Business Technologies
10.4.1	Critical systems have the correct and consistent time.	See all documents in 10.4			
10.4.2	Time data is protected.				
10.4.3	Time settings are received from industry-accepted time sources.				
10.5	Secure audit trails so they cannot be altered.				Orbility (OSP)
10.5.1	Limit viewing of audit trails to those with a job-related need.				Orbility (OSP)
10.5.2	Protect audit trail files from unauthorized modifications.				Orbility (OSP)
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.				Orbility (OSP)

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
					Business Technologies
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.				Orbility (OSP) Business Technologies
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).				Orbility (OSP) Business Technologies
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	***10.6*** *Review logs and security events for all system components to identify anomalies or suspicious activity.* ***Identify*** *the documented security policies and procedures examined to verify that procedures define reviewing the following at least daily, either manually or via log tools:* *• All security events.* *• Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.* *• Logs of all critical system components.* *• Logs of all servers and system components that perform security functions.* ***Identify*** *the documented security policies and procedures examined to verify that procedures define reviewing logs of all other system components periodically—either manually or via log tools—based on the organization's policies and risk management strategy.* ***Identify*** *the documented security policies and procedures examined to verify that procedures define following up on exceptions and anomalies identified during the review process.*	Policy and Operational Procedures	Log Management	Orbility (OSP) Orbility (OSP) Business Technologies
10.6.1	Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	See all documents in 10.4			
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.				
10.6.3	Follow up exceptions and anomalies identified during the review process.				
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	***10.7*** *Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).* ***Identify*** *the documented security policies and procedures examined to verify that procedures define the following:* *• Audit log retention policies.* *• Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online.*	Policy and Operational Procedures	Log Management	Orbility (OSP) Orbility (OSP) Business Technologies Business Technologies Business Technologies
10.8	Additional requirement for service providers only:	***10.8*** *Ensure that security policies and operational procedures for*	Policy and Operational	Information Security	Orbility (OSP)

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
	Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	*monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.* *Identify the document reviewed to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented.*	Procedures		Business Technologies
10.8.1	Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	See all documents in 10.8			
10.9	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.				Orbility (OSP) Business Technologies
	11: Regularly test security systems and processes				
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.	***11.1*** *Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.* *Identify the documented policies and procedures examined to verify processes are defined for detection and identification of authorized and unauthorized wireless access points on a quarterly basis.*	Policy and Operational Procedures	Vulnerability	Business Technologies
11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.		matrix	Inventory	Business Technologies
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.	***11.1.2*** *Implement incident response procedures in the event unauthorized wireless access points are detected.* *Identify the Incident Response Plan document examined that defines and requires response in the event that an unauthorized wireless access point is detected.*	Procedure	Incident Response	Business Technologies

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.	***11.2*** *Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).* *Identify the documented process for quarterly internal scanning to verify the process defines performing rescans as part of the quarterly internal scan process.* *I* ***dentify*** *the document reviewed to verify processes are defined for performing internal and external scans after any significant change.*	Procedure	Vulnerability	Business Technologies
11.2.1	Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.		Matrix	Inventory	Business Technologies
11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.		Procedure	Vulnerability	Business Technologies
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.		Procedure	Vulnerability	Business Technologies

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
11.3	Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.	***11.3 Best practice until June 30, 2015*** *Implement a methodology for penetration testing.* ***Identify*** *the documented penetration-testing methodology examined to verify a methodology is implemented that includes at least the following:* *• Based on industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network.* *• Testing to validate any segmentation and scope reduction controls.* *• Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.* *• Defines network-layer penetration tests to include components that support network functions as well as operating systems.* *• Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Retention of penetration testing results and remediation activities results.* ***Identify*** *the documented external penetration test results reviewed to verify that external penetration testing is performed:* *• Per the defined methodology • At least annually* ***Identify*** *the documented internal penetration test results reviewed to verify that internal penetration testing is performed:* *• Per the defined methodology* *• At least annually* *I* ***dentify*** *the documented penetration testing results examined to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.* ***Identify*** *the documented results from the most recent penetration test to verify that penetration testing to verify segmentation controls:* *• Is performed at least annually and after any changes to segmentation controls/methods. • Covers all segmentation controls/methods in use. • Verifies that segmentation methods are operational and effective, and isolate all out- of-scope systems from in-scope systems.*	Procedure	Vulnerability	Business Technologies
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).				Business Technologies
11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).				Business Technologies
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.				Business Technologies
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.				Business Technologies
11.3.4.1	Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.				Business Technologies

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	***11.4*** *Use intrusion-detection systems and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.* ***Identify*** *the vendor document(s) examined to verify defined vendor instructions for intrusion- detection and/or intrusion-prevention techniques*	Vendor Documentation	Network Policy	Business Technologies
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).				Business Technologies
11.5.1	Implement a process to respond to any alerts generated by the change-detection solution.				Business Technologies
11.6	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	***11.6*** *Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.* *Identify the document reviewed to verify that security policies and operational procedures for security monitoring and testing are documented.*	Policy and Operational Procedures	Information Security	Business Technologies
	12: Maintain a policy that addresses information security for all personnel				
12.1	Establish, publish, maintain, and disseminate a security policy.	***12.1*** *Establish, publish, maintain, and disseminate a security policy.* *Identify the documented information security policy examined.*	Policy	Information Security	Orbility (OSP) Business Technologies
12.1.1	Review the security policy at least annually and update the policy when the environment changes.	See all documents in 12.1			
12.2	Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.				Business Technologies
12.3	Develop usage policies for critical technologies and define	*12.3 Develop usage policies for critical technologies and define*	Policy	Employee Use	Orbility (OSP)

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
	proper use of these technologies. Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage. Ensure these usage policies require the following:	*proper use of these technologies.* *Identify the usage policies for all identified critical technologies reviewed to verify the following policies (12.3.1-12.3.10) are defined:* *• Explicit approval from authorized parties to use the technologies.* *• All technology use to be authenticated with user ID and password or other authentication item.* *• A list of all devices and personnel authorized to use the devices.* *• A method to accurately and readily determine owner, contact information, and purpose.* *• Acceptable uses for the technology.* *• Acceptable network locations for the technology.* *• A list of company-approved products.* *• Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.* *• Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.* *• Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.*			Business Technologies
12.3.1	Explicit approval by authorized parties	See all documents in 12.3			
12.3.2	Authentication for use of the technology				
12.3.3	A list of all such devices and personnel with access				
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)				
12.3.5	Acceptable uses of the technology				
12.3.6	Acceptable network locations for the technologies				
12.3.7	List of company-approved products				
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity				
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use				
12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.				
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	*12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.* *Identify the information security policy and procedures reviewed to verify that they clearly define information security responsibilities for all personnel.*	Policy	Information Security	Orbility (OSP) Business Technologies

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
12.4.1	Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.				Business Technologies
12.5	Assign to an individual or team the following information security management responsibilities:	***12.5*** *Assign to an individual or team to information security management responsibilities.* *Identify the information security policies reviewed to verify the specific and formal assignment of the following (including 12.5.1-12.5.5):* *• Information security to a Chief Security Officer or other security-knowledgeable member of management.* *• Responsibility for establishing, documenting and distributing security policies and procedures.* *• Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel.* *• Establishing, documenting, and distributing security incident response and escalation procedures.* *• Administering user account and authentication management.* *• Monitoring and controlling all access to data.*	Policy	Information Security	Business Technologies
12.5.1	Establish, document, and distribute security policies and procedures.				Business Technologies Orbility (OSP)
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.				Business Technologies Orbility (OSP)
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.				Business Technologies
12.5.4	Administer user accounts, including additions, deletions, and modifications.				Orbility (OSP)
12.5.5	Monitor and control all access to data.				Orbility (OSP)
12.6	Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.				Business Technologies SP+ DEN Parking & Transportation Orbility (OSP) Orbility (OSP)
12.6.1	Educate personnel upon hire and at least annually. Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.				Business Technologies SP+ DEN Parking & Transportation Orbility (OSP) Orbility (OSP)
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.				Business Technologies SP+ DEN Parking & Transportation Orbility (OSP) Orbility (OSP)
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)				Business Technologies SP+ DEN Parking & Transportation Orbility (OSP)

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
	Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.				Orbility (OSP)
12.8	Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows				DEN Parking & Transportation
12.8.1	Maintain a list of service providers including a description of the service provided.				DEN Parking & Transportation
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.				DEN Parking & Transportation
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.				DEN Parking & Transportation
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.				DEN Parking & Transportation
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.				DEN Parking & Transportation
12.9	Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.				DEN Parking & Transportation
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.				Business Technologies

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
12.10.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.				Business Technologies
12.10.2	Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.				Business Technologies
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.				Business Technologies
12.10.4	Provide appropriate training to staff with security breach response responsibilities.				Business Technologies
12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.				Business Technologies
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.				Business Technologies
12.11	Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.				Orbility (OSP)
12.11.1	Additional requirement for service providers only: Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.				Orbility (OSP)
	A1: Additional PCI DSS Requirements for Shared Hosting Providers				

ID (3.2)	REQUIREMENT (3.2)	*Testing Procedure*	Typical Document Type	Functional Classification(s)	Responsible Party
A1	Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.	*n/a*			n/a
A1.1	Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	*n/a*			n/a
A1.2	Restrict each entity's access and privileges to its own cardholder data environment only.	*n/a*			n/a
A1.3	Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	*n/a*			n/a
A1.4	Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	*n/a*			n/a
	A2: Additional PCI DSS Requirements for Entities using SSL/early TLS Note: This Appendix applies to entities using SSL/early TLS as a security control to protect the CDE and/or CHD				
A2.1	Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either • Confirm the devices are not susceptible to any known exploits for those protocols. Or: • Have a formal Risk Mitigation and Migration Plan in place.	*See 2019 Compensating Control Worksheet*			Business Technologies
A2.2	Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.	*See 2019 Compensating Control Worksheet*			Business Technologies
A2.3	Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June 30, 2016. Note: Prior to June 30, 2016, the service provider must either have a secure protocol option included in their service offering, or have a documented Risk Mitigation and Migration Plan (per A2.2) that includes a target date for provision of a secure protocol option no later than June 30, 2016. After this date, all service providers must offer a secure protocol option for their service.	*See 2019 Compensating Control Worksheet*			Business Technologies

Exhibit F
Pre-Assessment Evidence

ID	Evidence Type	Explanation	Relevant Requirement Sections	Responsible Party
E1	**Network Configurations**	Be prepared to provide current production configurations for all in-scope Network Components. This may include the following sub-types: Firewalls Routers	1.X 2.X 10.4 11.4	Business Technologies Business Technologies
E2	**ACL Reviews**	Provide the results from the two most recent firewall and router ACL reviews (bi-annual). This should include all information from the review and examples include: Date	1.1	Business Technologies Business Technologies
E3	**Mobile and Employee Owned Devices**	Unless is was fully documented in the **CDE Inventory** be prepared to provide a list of all mobile and employee owned devices that can access the CDE.	1.4	Orbility (OSP)
E4	**Component Configurations**	You may be able to provide the current production configurations for all sampled in-scope components. This includes all component types not covered in E1 (Network Components).	2.X 3.2 3.4.1 4.1 5.1 6.2 6.6	Orbility (OSP) Business Technologies Business Technologies Business Technologies
E5	**Removable Media**	Provide a representative list of removable media types that are used to store cardholder data. The typical example here would be backup tapes. Please indicate all locations where removable media types can be stored.	3.4	Orbility (OSP)
E6	**Wireless Networks**	Identify all in-scope wireless networks transmitting cardholder data or connected to the cardholder data environment.	4.1.1	n/a
E7	**Custom Application Changes**	Provide a list of all recent custom code changes for all in-scope applications. Coalfire will select a sample of these changes for review.	6.3.2 6.4.5.3	Orbility (OSP)
E8	**Change Control Documentation**	Be prepared to provide change management documentation that correlates to observed changes on any Coalfire sampled system components.	6.4.5	Orbility (OSP) Business Technologies Business Technologies Business Technologies

E9	**Secure Development Training**	Provide evidence that software developers received training on secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.	6.5	Orbility (OSP)
E10	**Web Application Vulnerability Security Assessments**	If Web application vulnerability security assessments are used to meet requirement 6.6, provide the final report for each current report associated with all in-scope web-facing applications.	6.6	Orbility (OSP)
E11	**Terminated Users**	Please provide a list of all users that we're terminated within the last 6 months. Preferably, these are users who would have had access to in-scope systems or connected systems. Coalfire will select a sample of these users for review.	8.1.3 9.3	Business Technologies SP+ DEN Parking & Transportation Orbility (OSP) Orbility (OSP)
E12	**Access to Physical CDE**	Provide a list of onsite personnel with physical access to the CDE. Coalfire will select a sample of these personnel to interview for this requirement.	9.3	Business Technologies Orbility (OSP)
E13	**Media Movement Records**	If removable media is transported to/from data centers, we'll need to review a sample of recent media movement records.	9.6.2	Orbility (OSP)
E14	**Media Inventory Results**	Provide the results from all removable media inventories performed over the prior year.	9.7.1	Orbility (OSP)
E15	**Risk Assessment Documentation**	Provide all relevant Risk Assessment documentation from the previous year for review	10.6.2 12.2	Business Technologies
E16	**Wireless Scanning Results**	If wireless scanning is used to meet requirement 11.1, provide the last 4 quarters of scan results for all in-scope locations.	11.1	Business Technologies
E17	**Wireless Access Point Inventory**	Provide the current inventory that identifies all wireless access points.	11.1.1	Business Technologies
E18	**Internal Vulnerability Scans**	Provide the reports of all internal vulnerability scans that have occurred over the last 12 months. If tracking utilities or spreadsheets are used to ensure resolution of identified vulnerabilities, provide these as well.	11.2.1	Business Technologies
E19	**External Vulnerability Scans**	Provide the ASV scan reports for all external vulnerability scans that have occurred over the last 12 months.	11.2.2	Business Technologies

E20	**Penetration Test Results**	Provide the internal external penetration testing reports for the current year. If significant changes were made to the in-scope environment, provide the penetration testing results associated with those changes as well.	11.3	Business Technologies
E21	**Reported Incidents**	Provide a list of all reported incidents or alerts over the last 12 months. Coalfire will select a sample (if appropriate) for reviewing against this testing procedure.	12.10.1	Orbility (OSP) Business Technologies Business Technologies Business Technologies
E22	**Compensating Control Worksheets**	Provide documentation for all planned uses of compensating control worksheets (CCWs). If you have used CCWs in previous year's assessments, they may be provided as a baseline; however, they will need to be updated to reflect the current environment. Please ensure you provide and entry for each of the following: • **Constraints:** List constraints precluding compliance with the original requirement. • **Objective:** Define the objective of the original control; identify the objective met by the compensating control. • **Identified Risk**: Identify any additional risk posed by the lack of the original control. • **Definition of Compensating Controls**: Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any. • **Maintenance:** Define process and controls in place to maintain compensating controls.	CCW	Business Technologies

Exhibit F
Technology Identification

ID	Technology Type	Explanation	Relevant Requirements	Responsible Party
T1	**Personal Firewall Software**	Identify all personal firewall software used on any mobile and/or employee-owned devices.	1.4	Business Technologies Orbility (OSP)
T2	**Administrative Access Methods**	List out all non-console administrative access methods including the encryption used to protect these connections. This needs to cover how connections are made to all in-scope system components. Examples Include: SSH2 using AES 256-bit SSLv3 HTTPS	2.3	Business Technologies Business Technologies Orbility (OSP) Business Technologies Orbility (OSP)
T6	**End User Messaging Technologies**	If applicable, list all End User Messaging technologies used to transmit cardholder data(for example, e-mail, instant messaging, chat, etc.).	4.2	Orbility (OSP)
T7	**Anti-Virus/Anti_Malware**	Identify all anti-virus and anti-malware technologies in use.	5.1	Orbility (OSP) Business Technologies
T8	**Change Management Software**	If tracking software or systems are used to support the Change Management process, please identify them here.	6.4.5	Business Technologies
T9	**Web Application Firewall**	If a Web Application Firewall (WAF) or other automated technical solution is used to meet requirement 6.6 identify the technology(ies) here.	6.6	Orbility (OSP)
T10	**Two-Factor Auth**	Identify any two-factor authentication solutions used for remote network access originating from outside the network, by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance). Include all remote-access technologies associated with the CDE.	8.3 12.3.8	Business Technologies
T11	**Time Synchronization**	Identify the time synchronization technologies in use. (If NTP, include version)	10.4	Business Technologies
T12	**Log Correlation and Review**	Identify all log protection, correlation and review utilities.	10.5 10.6 10.7	Business Technologies Orbility (OSP) Orbility (OSP)
T15	**Internal Vulnerability Scanning**	Tool or Vendor used to conduct internal vulnerability scanning.	11.2.1	Business Technologies