RFP #3372-5 ADDENDUM #1
&
ACKNOWLEDGMENT OF RECEIPT

Description: **Districtwide Managed Print Services, Equipment Repair & Maintenance and Onsite Services**

RFP #: 3372-5 Addendum #1
Date: April 14, 2017

This addendum includes the following information:

Below are responses to some of the questions that were received. If your question was not specifically answered it is because we felt the question was not pertinent to your ability to respond to the RFP, it did not address what we are requesting in the RFP, it is information that only the successful proposer will need and can be obtained when they start working on the project, and/or the answer is already in the RFP package or available on our web site. ***NO FURTHER QUESTIONS WILL BE ACCEPTED OR ANSWERS PROVIDED.***

A. Responses to some of the questions received are as follows:

Section 2.3

Q: Please confirm the number of printed copies the District would like to receive. RFP Section 2.3 states "The Proposal packet must contain one (1) original, eight (10) copies of the proposal and one (1) copy in PDF Format on a USB flash drive.

A: Please submit (10) copies of the proposal.

Section 4.2.1.3 Large Format/Plotting Devices

Q: How many units currently need to be replaced inside your current fleet of large format printers? Any Vendor

A: Unknown at this time. Units will be purchased on an as needed basis.

Q: Do you have scanning needs in any departments that use a large format device?

A: See previous answer

Q: Would you prefer pricing on 3 or 5 years of service?

A: Please provide pricing per the contract terms listed on page 7, Section 2.12.

Section 4.2.1.4

Q: Is it acceptable to produce medium to high volume, books, mailings, fliers and other higher volume work at a separate production other than the copy center for cost savings?

A: Yes.

Section 4.2.1.5.1

Q: Current equipment by specification (what is owned versus what will need to be replaced)?

A: Owned; will be replaced on an as needed basis.

Q: Turnaround time requirements?

A: Incoming mail is delivered to each campus or location by USPS. The mail is then sorted by either supplier staffed mailroom employees or MCCCD employees. The mail is them distributed to individual departments and/or mail drop boxes. The current supplier, at times, may deliver mail along with copy center print jobs through each day. Outbound mail may be collected during these times for daily pickup by USPS. The awarded supplier is responsible for meeting delivery times and schedules to meet the needs of the individual campuses and district office.

Q: Pick-up and delivery routes?

A; Mail delivery and pickup routes at each campus will be provided to the awarded supplier.

Section 4.2.1.5.3

Q: What is the current workflow utilized for the variable data jobs submitted today?

A: Varies by campus. Email. Online submission.

Q: Are all variable data jobs performed in one location or at each college? Is the process standardized from College to College?

A: Each college. No.

Q: In the RFP there are references to documents being finished, does MCCCD own the finishing hardware?

A: The existing supplier owns all finishing equipment in the copy centers, with a few minor exceptions.

Q: Can you provide of list of "off-line" finishing equipment utilized at each location?

A: Typically, each campus provides at minimum Coil Binding, Laminating, Cutting and Folding... some campuses also offer Drilling, Padding, Shrink-wrap

Q: Is there a list of the finishing hardware used in the copy centers?

A: See previous answer

Section 4.2.1.5.2

Q: The RFP document indicates prodding Shipping & Receiving services but does not provide any volumes of inbound or outbound shipping. Can you provide volumes for each location?

A: Shipping & Receiving is not done through this contract at all colleges and locations, but is limited to the colleges that choose to leverage this service.

Q: Is there a campus wide shipping tools utilized for outbound shipping or is it the responsibility of the Shipping/Receiving staff to process outbound shipments?

A: No

Section 6

Q: Is there percentage for each of the areas as it relates to the evaluation of proposals? Ex: Page 25 section: 6.1 and 6.2 list all criteria – will one be more important than the other?

A: Evaluation criteria is stated on page 25 of the original RFP. A breakdown of points, percentages or scoring will not be provided prior to award.

Q: Will any request to alter or add conditions to MCC terms and conditions automatically disqualify a bidder?

A: MCCCD allows exceptions to the RFP terms and conditions, but this does not constitute acceptance - Exceptions will be negotiated as part of the contract

Q: Section 3 on page 8 and section 4.3 on pages 22-23 read such that No Exceptions can be made to the General Terms and Conditions contained in the RFP, however on page 27, it states that Offerors may submit pricing based off of existing cooperative contracts. Does Maricopa intend to leverage a cooperative contract for procuring products and services under the RFP? If yes, please confirm that the terms and conditions of an existing cooperative, if used, would govern and not the General Terms and Conditions contained in the RFP and whether incorporating such terms and conditions in our response would be characterized as an exception making us non-responsive?

A: MCCCD allows submission of cooperative contracts primarily to access the associated pricing of those contracts. Terms and conditions of the cooperative contract that differ from the MCCCD RFP terms and conditions will require legal review and possible negotiation.

Q: Is MCCCD looking for the bidder's quote of the total amount of equipment, supplies, service, head count, technology and professional services they recommend to perform all of the functions required to manage the entire scope of the future-state program? Or is MCCCD looking for a "catalogue" of items with associated pricing in each of the categories to give MCCCD an idea of cost based on projected levels in order to make an informed selection and then allow the successful bidder an opportunity to assess the various service areas and make an informed recommendation at that time in order to provide MCCCD the greatest favorable impact in cost savings and productivity?

A: Proposals can be submitted for one, some or all of the areas outlined in the RFP.

Q: Is there a common format MCCCD would like the pricing responses submitted in?

A: No, but MCCCD is not requesting a "lump sum" price sheet, therefore, pricing for goods and services should be broken down according to section and/or type and by campus/college.

Q: Do the 50 pages exclude the addendums A, B, C, and D mentioned in (Section 8)?

A: MCCCD is eliminating the 50 page limit on this RFP.

Q: Is it the intent of MCCCD to purchase only "new" equipment that has never been previously sold (i.e. remanufactured, newly remanufactured or certified used)?

A: Suppliers should submit pricing on new equipment only.

Q: Can you provide floor plans for all campuses?

A: This information is not currently available.

Q: After deleting any financial or incumbent information, can you provide the Statement of Work and Service Level Agreements for all campuses?

A: No. Volume and workload varies by campus. Please refer to the services listed on pages 1-3 on the "MCCCD Ricoh Services Spreadsheet 3372-5.pdf" file.

Q: The pricing section page 27 references Attachments A, B and C. Are your providing us pricing forms to fill out or you would just like us to label our own excel pricing documents as such?

A: Please submit detailed pricing schedules for each section and label them as stated.

Q: Are student workers employed in any of the Onsite Services staffing areas, to maintain current operations?

A: No, but MCCCD is open to utilizing student workers.

Q: Is your current fleet of copiers/MFP's (Ricoh) owned by MCCD or are they on lease?

A: MCCCD owns all devices.

Q: If any or all of the units are on lease can you provide lease-end and payment information on the leased assets?

A: At the present time, it is believed that MCCCD does not have any leased equipment.

Q: Is the District looking to refresh all MFP's once the bid is awarded or are you looking to phase in new MFP's on an "as needed basis"?

A: Campuses will replace equipment on an as needed basis, each college may vary.

Q: If you are considering the "as needed" phased approach would it be the District's expectation that the winning bidder support the current fleet of Ricoh units or would your current vendor support those until the units are phased out?

A: It is MCCCD's preference that the awarded supplier will maintain the existing fleet of MCCCD owned MFDs and printers, however, if this is not possible, MCCCD will continue utilize the existing service provider.

Q: Also in the phased approach option, can you give any rough numbers on a year-over-year implementation schedule to phase out the legacy equipment?

A: No, campuses will replace equipment on an as needed basis, each college may vary.

Q: The scope of work is clear that the winning bidder must be able to provide on-site personnel to run the copy centers, mail rooms and shipping/receiving operations at each campus. What is the current personnel headcount for the operational staff provided by your current vendor across the district?

A: The awarded supplier will be responsible for providing adequate staffing to meet the needs of each campus and districtwide.

Q: Has that count been sufficient to meet the District's needs and if not what number would the District like to see provided by the winning bidder?

A: The current staffing level have been sufficient, but it is up to each supplier to provide a staffing proposal that meets the demand for each campus.

Q: How many vendor-provided staff need to have fork lift certification?

A: The awarded supplier is required to have a minimum of (1) fork lift certified staff essential for performing these duties during normal business hours at each supplier staffed shipping and receiving department at each participating campus.

Q: Does the current personnel have any type of "non-compete" agreement that would preclude them from being recruited by a competing vendor that you know of?

A: Unknown.

Q: Did MCCD utilize a consultant for crafting this RFP and, if so, are you open to disclosing who the consultant is?

A: There is no consultant for the RFP.

Q: For the Managed Print Services (MPS) support is it mandatory that the successful bidder provide OEM supplies?

A: No

Q: Is there a current secure print solution in place on campus?

A: Varies by campus.

Q: Is there an existing payment gateway that needs to be utilized by the solution offer? If Yes what is the current payment gateway?

A: Not all colleges have a payment gateway, but it may vary from college to college.

Q: Print related reporting capability related to devices, users, documents, usage, cost, historical perspectives, etc. How many Users/Students/Faculty will need to be tracked for reporting?

A: Unknown

Q: What does RSC and MCOR have for equipment and services? Nothing is listed on the spreadsheet.

A: MCOR no longer exists as a standalone campus. MCOR is now part of Rio Salado College (RSC). RSC does not list equipment because they have historically not participated in the contract. RSC may participate in the contract.

Q: What services does each campus want? Do they want the same services they receive today or something different?

A: This will vary based on each college. Plan on the same exact services being provided as they presently are; however, each college will vary.

Q: What period of time was used to develop the average monthly volume?

A: Data provided on the "MCCCD Ricoh Services Spreadsheet 3372-5.pdf" file is based off of one (1) quarter of usage and broken down into estimated monthly usage.

Q: What does the minimum monthly cost consist of, i.e. equipment base fee, full services maintenance base fee, etc.?

A: Please refer to the services listed on pages1-3 on the "MCCCD Ricoh Services Spreadsheet 3372-5.pdf" file.

Q: Do each of the locations have outbound mail machines w/meters for processing outbound mail? If yes, can you provide the Manufacturer and Model Numbers?

A: Yes; current supplier passes through meter rental and maintenance cost for Phoenix College (Pitney Bowes) and Mesa Community College (Neopost)

Q: Are the copy jobs and mail delivered to a central location for user pick-up or is it delivered desk to desk?

A: Varies by campus.

Q: How are packages handled at each location? Do the private carriers (UPS, FedEx) deliver to each building or recipient or are they delivered by the mail staff?

A: Packages are delivered to the Receiving dock and distributed by the Receiving staff.

Q: Are the hours of operation listed in the MCCCD Ricoh Services spreadsheet the College operating hours or those of the Copy and Mail Center operations?

A: Service hours required to serve the needs of each campus. Coverage is required during these campus operating hours.

Q: Will you validate the individual copy center print volumes for each location? There appears to be some inconsistencies with the equipment list average monthly volumes and the estimates provided in the table of College location services.

A: Copy center volumes are based on average impressions per month.

Q: Is the Delivery and Pick up Schedule the actual mail route for each location that includes delivery of copy jobs and paper?

A: In most cases all orders are delivered per scheduled delivery runs, but customers also pick up.

Q: What types of off-line finishing requirements are there for the copy jobs produced?

A: Folding by hand, Saddle stich, Binding (combs, spiral and metal combs), Collates by hand, Cutting, Laminate, 2-hole punch, MCD padding, Glue padding, Shrink wrap, Scanning, Placing print jobs into 3-ring binders.

Q: What are the volumes of off-line finishing functions performed in the copy center? (Example, # of comb or spiral binds, cutting, laminating etc.)

A: Example provided for District Office: Folding by hand - 2607/week, Saddle stitch - 1000/month, Binding - 200/month, Collated by hand - 150/month, Cutting with cutting board - 250/week, Laminate - 200/month, 2-hole punch - As Requested, NCR Padding -150/month, Glue Padding - 100/month, Shrink Wrap- As Requested, Scanning - 8000/month, Placing print jobs in 3-ring binders - As Requested.

Q: How often are the routes run and what times for all locations?

A: Most campuses pick up mail twice a day; here are the current pickup times for the District Office locations as reference:
District Office- 9:00 am and 3:00 pm.
Emerald Point- 9:15 am and 3:00 pm.

Q: Does the MFD's, Printers, or Copy Center equipment come with any impressions, if so how much? Please break it down per device.

A: MCCCD pays per click with a minimum monthly cost

Q: Professional Services for Software Install and Set Up. Is Remote installation and training of the solution need or onsite?

A: This may vary by product, and should be up to the party who is currently entering in contract for that purchase

Q: If Onsite installation and training is required how many Admins will need trained on the solution?

A: Minimum of two

Q: Will configuration of the solution be required on all devices?

A: Configuration requirements, if any, will be provided to the awarded supplier.

Q: What is intelligent device monitoring?

A: This would refer to SMNP monitoring of all networked products. This may also extended to log files exporting if possible.

Q: What is remote enterprise pro?

A: Please refer to the service level agreement provided.

Q: What is the definition of fleet management services?

A: Providing service to the printers on contract, including providing paper, toner, maintenance, repair, etc.

Q: What is the definition of printer fleet services?

A: Providing service to the printers on contract, including providing paper, toner, maintenance, repair, etc.

Q: Are there any common features that are on all or most of the MFD's and printers?

A: A list of manufacturer name and model is provided on the "MCCCD Ricoh Services Spreadsheet 3372-5.pdf" file.

Q: Is there an electronic package tracking system being utilized today for accountable mail and/or packages?

A: No

Q: How are job requests submitted to each of the Copy Centers? Is there a Web Submission tool used today? Is each College different or is the submission process standardized across all colleges?

A: This may vary by site, but the central method is the use of a vendor-supplied job submission application/portal.

Q: What is the configuration for each piece of equipment?

A: Configuration requirements, if any, will be provided to the awarded supplier.

Q: Is MCCCD open to software solutions that are SAAS or does the software have to reside within the MCCCD network?

A: No, SAAS or cloud-based solutions are also acceptable. On-premise is not a requirement

Q: What ERP/SIS do you use? Is the same ERP/Student Information System used across all campuses?

A: Oracle PeopleSoft

Q: Do you have a document management or Enterprise Content Management platform in place today? If yes, what platform do you use?
Is it used across all campuses?
Is it deployed across all departments or only a subset of departments?

A: On a campus-by-campus basis. At least three sites are now using Kofax and EMC AppEx platforms for document management, for example

Q: Does MCCCD interact with your current Document Management Solution? If no, is there a specific reason? Would you consider it in the near future?

A: Currently campus purchased, managed, and controlled

Q: Can you elaborate on "Without utilizing third-party application"? ·Integrated Mobile device printing capability (from any BYOD device to any allowed printer), without utilizing third-party application.

A: The supplied solution should be all-inclusive, without necessitating additional procurement of third-party mobile printing capability. We really don't want to have a client/agent software requirement if possible.

Q: Will MCCCD allow for the installation of a software client on the workstations to indicate to the end user of the rerouting?

A: That is dependent on what you are "rerouting"? We would like to refrain from client/agent software where possible, but this has been a decision made at the campus level. In some cases of print management, we have opted to allow for an agent software to reroute jobs.

Q: Which of the following methodologies does MCCCD want to print with mobile devices:
i. Upload a file to a MCCCD web Page
ii. Via an MCCCD email address . i.e.. print@mccccd.edu
iii. Via an email address outside of MCCCD's network, i.e. Hotmail, Gmail, Google, MSN, etc.
iv. Via downloading an app to your iPhone. IPad, Android, blackberry. Etc.?

A: Submit all possible options for consideration.

Q: Print related reporting capability related to devices, users, documents, usage, cost, historical perspectives, etc.- including real time administrative dashboards

h. Does MCCCD want administrators to view these reports at each campus?

i. Do these need to be web based reports?

A: h. MCCCD would like for admins at each campus/location to be able to view reports. i. Web-based would be preferable

Q: Ability to directly download and install updates, etc. directly from vendor

i. Will MCCCD perform the updates or do you want one of our staff members to be available to assist with this?

j. Do you require that these hotfixes/updates be performed after hours or on weekends?

A: i. MCCCD should have the option to directly download and install updates. If vendor assistance is needed, arrangements can be made with the vendor; including any scheduling concerns. We do not want to be locked into having to go through the reseller to acquire access to software, patches and/or licensing. All purchase contracts should allow for the college and/or district to decide if they would like to self-manage their installations and products without having to communicate with the VAR, or need to involve them on helpdesk tickets. Autonomy is a requirement. j. It is up to the site as to when the patching is performed.

Q: Monitored print solution, with automatic notification

k. What type of notifications are you requiring?

A: Detail what types of notifications your solution provides.

Q: Secure printing, copying or scanning

m. Regarding scanning, which of the following features are a requirement:

i. Scan to users email

ii. Scan to network folder

iii. Scan and email to outside email address directly on MFD

1. Do you require that a "sent email" be duplicated on the user's actual email exchange box?

iv. Scan to document managing solution . If so, which ones…

v. OCR document and convert them to Word, Excel, PowerPoint, etc.…

vi. Does MCCCD require a "Single sign on" solution when accessing all the features of the MFD?

A: m. i. Yes ii. Yes iii. Yes 1. No, but could vary by sites preference. iv. No, not required v. No, not required vi. Can vary by site, and not a requirement

Q: Does MCCCD have Sequel Servers that they want our databases to reside on or do you want vendor to provide our own sequel databases?

A: MCCCD has their own servers for the SQL databases, and will be responsible to securing access to those resources

Q: Can MCCCD provide 2 VM servers per Campus to be utilized as a Print Server and as a Mobile Print Server? These can be 2008,2012, 0r 2016 servers.

a. Can MCCCD IT manage these servers?

A: Yes to both questions.

Q: Does MCCCD require that all campuses data be compiled at a centralized database or can each campus control and manage their own data?

a. If a centralized data server is required, what type of network infrastructure cabling is between each campus? i.e. Fiber optics, T1, Vlan, etc..

A: Not required, and may not be possible. Each site is capable of managing their data. a. Each campus is separated by a 200Mpbs (minimum) WAN connection between sites.

Section 4.2.1.4

Q: Requests "on-site technical support" Please define the role of this support.

A: Support of printing devices (toner, paper, jams, moves), print solutions, etc.

Q: Please describe how the current on-site support is being delivered. Is there a full time person at each campus? Is this person a fully trained technician or just someone who provides initial response to any issue like out of toner, paper, jams etc. and then dispatches a fully technician if it is something more.

A: Can vary by campus. The initial response is generally completed by the sites IT department, and then escalated to the copy center for further work by a technician. In most cases the copy center is not staffed by anyone who has a technical support background.

Q: How many full and part time employees are provided by the current vendor

A: Proposals should include adequate staffing based on the information listed in the RFP.

Q: Does MCCCD find the support to be adequate, insufficient or overstaffed

A: MCCCD cannot provide an answer for this question.

Section 4.2.1.3

Q: What language are you printing? Standard List: HP-GL/2, HP-RTL, TIFF, JPEG, CALS G4, HP PCL 3 GUI, URF (IS Post Script Needed)

A: PCL and Postscript. We have a lot of Mac throughout the district, and they still rely on PS drivers in most cases

Q: What is the maximum volume per month printed on any current device? EX: 3,000 sq. feet a month

A: Current data is not available, as it varies from each college, building, area of the organization

Q: What is the minimum and maximum width you would need for wide format devices? EX: 24 , 36, 42, 44, 60 IN width

A: 36" width should be sufficient for most plotting of drawings (30x42 in portrait mode). As long as the plotter can rotate a document wider than 36" to print it longer in the direction of the paper path.

Q: What applications are you using for large format prints? EX: Illustrator, CAD Design, Bently, Ativa

A: AutoCAD, Illustrator, Excel, Word, some .jpg/.gif/image files. The issue recently has been the memory in the plotter as it loads and processes a print job. Our documents are getting denser in information and printing multiple sheets in a single print request tends to choke our current plotter, so we end up having to print sheets 1-6, then 8-12, etc. Our plotter also serves as a scanner for large scale documents, sending the scan into our server files.

Q: When printing is 2400X1200 optimized DPI the standard?

A: 2400x1200 is extreme end of output and costly depending on type of plotter. There's not a lot we do at the very high point density as we try to increase printer speed and save toner.

Q: What is the minimum speed per page for an A1 or D Size Drawing?

A: Speed shouldn't be an issue with the page size noted unless a large volume of copies or many pages are typically planned to be plotted. Also depends on image resolution being plotted.

Section 4.2.1.4.1

Q: Please fully describe the Pay for Print Solution as it currently is today and the desired state.

A: Equitrac Express. Works, but open to other products. Would be disruptive in several cases throughout the district to change providers due to concentration, training, licensing and device investment.

Q: Does MCCCD own any of the equipment in the print shop(s). I.e.. cutters, drill press etc. Please define all services offered by the Print Shop.

A: Supplier staffed copy centers contain equipment which is supplied by the supplier.

Q: How many non MCCCD staff members are operating the print centers and what are their responsibilities.

A: Total Non-MCCCD, supplier provided staff members are (39) District-wide (including on-site management, copy/print, mail, fleet management, receiving and etc.)

Q: Does MCCCD outsource any printing and is there a desire to bring that in house. If so what is being outsourced.

A: MCCCD outsources a significant amount of printing, not considered "copy center" print jobs. There is no current desire to bring these print jobs in-house.

Q: Is there couriering of print jobs and if so who does this. Is this refined to on campus or are jobs being couriered between campuses.

A: MCCCD has courier services for intercampus mail delivery throughout the district.

Q: Who currently provides the mail services and is this integrated in any way with Print Shop operations.

A: Please review the "MCCCD Ricoh Services Spreadsheet 3372-5.pdf" file to review campuses that utilize Ricoh staffed mailroom services.

Q: Does MCCCD own a Managed Print Solution Software Application like PaperCut? Has MCCCD investigated these solutions and has a current preference.

A: MCCCD does not have a unified Managed Print solution. It varies based on each college.

Q: Does MCCCD use a leased solution currently and if so what is the product. How many users, either currently use or would use this solution. How many servers would this solution sit on. How many MFP's would this solution need to be integrated into.

A: MCCCD does not currently have a leased solution.

Q: Does MCCCD currently have Integrated Mobil Device printing capability and if so what.

A: MCCCD does not have a unified Managed Print solution. It varies by site

Q: The request is for a mobile printing solution without using a third party app. like Air Print etc. Please provide an example of a known solution that meets this requirement.

A: MCCCD is asking suppliers to provide known solutions.

Q: Please define/ describe what Direct technical support for print related services look like to MCCD.

A: Printer repair, paper jams, toner, moves, configuration, security, etc.

Q: Is there a student pay card system in place today? If so are we, a) taking over the management of that system, b) interfacing our technology with that system? Please describe the details regarding any student pay cards. Or are we installing a new system.

A: Yes, however it varies based on each college as there is no unified print management solution across MCCCD. a) No, you are not taking over the management of those systems. b) No

Q: Does MCCCD currently use a solution like Blackboard for students, staff and faculty?

A: Canvas by Instructure

Q: Who will be using this service, the general public or just faculty, staff and students.

A: Mobile printing can be utilized by all listed.

Q: Does MCCCD use some e sort of smart / HID or proximity card which could be leveraged with this solution? If so please define.

A: MCCCD has various proximity card solutions throughout. Each site may use a different methodology or hardware solution

Q: How many devices would need to have a credit card solution?

A: Any MFD's in public use areas will require a credit card solution.

Q: Would these need to be color?

A: Yes

Q: What solution is currently being used to meet this requirement?

A: Currently, we do not accept credit/debit cards to deposit onto p4p accounts.

Q: How many devices across all campuses are set up with this solution?

A: Unknown

Section 4.2.1.5.1

Q: Reporting requirements?

A: We need the functionality/data to charge each department for usage. This should be in an easy to access report

Q: Content/document/job submission methodology?

A: I believe this was answered on line 21. I would add that some instructors send in/drop off hard copies.

Q: Electronic storage requirements?

A: The only Electronic storage I know if is for Document imaging.

Section 4.2.1.4.1.5

Q: Please describe what is in place today.

A: 1. Maricopa is in the process of researching and acquiring a new help-desk software system. Until that is completed by the summer of 2017, there are no integrations currently available, but, it is expected that in the future whatever new system is acquired will have an API to support such activity. At that time, it would be the assumption that the selected vendor would support whatever API is available.

Q: How many staff members are required at each campus and or administrative locations?

A: The awarded supplier will be responsible for providing adequate staffing to meet the needs of each campus and districtwide.

Q: What are their duties and responsibilities?

A: 1. If this is really about staff augmentation, then: Help-desk responsibilities vary from college to college. Some support both staff and student tier I questions, while others support one group or the other. Some help-desk team members leave their area and go help employees with their technology issues while others never do. Again this is a question for the colleges if you want specific or detailed answers.

Q: Please define if there are locally connected devices (printers connected via USB etc.) throughout the organization and how MCCCD wishes to have these supported.

A: We do not wish to have these supported. Support for USB desktop printers varies by campus, and some cases may not be allowed.

Q: Variable Data Printing - Please describe what solutions are currently being used to accomplish this task and if MCCCD owns the solution. What device(s) are these currently being output to and does MCCCD own these devices?

A: MCCCD is asking suppliers to provide known solutions. Detail what your solution provides.

Q: Is there a requirement for MICR (magnetic toner for check printing) printing?

A: Yes

Q: What is the volume of GBC and Coil bind. Is this being done off line or in line to any extent? What if any equipment does MCCCD own that would assist with these requirements?

A: The awarded supplier will be responsible for providing any and all equipment required to meet the needs of each campus and districtwide.

Q: Is this required at each campus?

A: Yes, for any campuses requiring these services.

Q: Does MCCCD currently have any sort of job submission software solution which allows users to remotely submit requests for printing to a centralized print shop that then has the ability to charge the user via Blackboard, credit card or other? What choices other than coil and saddle stich are offered? Color paper, special stock for covers etc.

A: Yes, but it is provided by the vendor who manages the print shop.

Q: Who supplies the paper and specialty stock, coils etc. etc.?

A: The existing supplier provides all paper, specialty stock and binding materials at all campuses except EMCC and SCC

Section 4.2.1.6.1

Q: Please further outline the required scanning solutions. Does this just refer to the multifunction devices ability to perform this task?

A: MCCCD is asking suppliers to provide known solutions. Detail what your solution provides.

Q: Is MCCCD using any integrations solutions today such as e-Copy? If so how many devices need to have this ability?

A: MCCCD is asking suppliers to provide known solutions. Detail what your solution provides.

Q: What Document Management Solution (electronic filing) is MCCCD currently using?

A: It varies based off each college, MCCCD is using Hyland, but other colleges are using Fortis/Kofax or another solution. MCCCD is working to consolidate into a single solution

Q: Is any special integration required or is this just a standard application that the device be able to scan to SMB or e-mail?

A: MCCCD is asking suppliers to provide known solutions. Detail what your solution provides.

Q: Attachment A, Bidder References states "MCCCD requires a minimum of five (5) current and local references for which you are providing same or similar products and services specified herein." However, the form provides space for 3 companies. Please confirm the number of references the District wants vendors to provide.

A: Replace old attachment with revised Attachment A

Q: Attachment C requests vendors to "select the correct drop-down box entry for each of the following report types"; however, the PDF does not show the choices available from the drop-down list. Can you please provide the native version of this form or list the selections response options for each report type?

A: Replace old attachment with revised Attachment C

B. A Request For Proposal is a document we use when we are looking for companies to submit proposals that explain what their capabilities are, what services they offer, and various pricing schedules for different types of services offered. We have given you, to the best of our ability, an outline (Scope of Work in Section 5 of the RFP) of what we are looking for. You, not MCCCD, are the experts in providing these services to organizations like ours and you have the knowledge and expertise we are looking for. We expect you to submit a proposal that gives specifics of your company and what services you can offer MCCCD in response to the needs expressed in this RFP.

C. **The Proposal Due Date HAS BEEN CHANGED to:**

1. **Due Date: Tuesday, May 16, 2017 3:00 P.M. (Local Time)**

THERE ARE NO FURTHER CHANGES TO THIS ADDENDA

END OF ADDENDUM NO.1

Please fill in the requested information below as acknowledgment that you have received this addendum as noted above. **Please include a signed copy of this Addendum Acknowledgment IN YOUR PROPOSAL when it is submitted.**

Name of Firm: _____

Address: _____

_____

Fax # : (_____)_____ Tel. #:(_____)_____

Name :(Print) _____Title: _____

Signature: _____Date: _____

E-Mail: _____

ATTACHMENT A

BIDDER'S STATEMENT (continued)

BIDDER REFERENCES

Private Business Contracts

MCCCD requires a **minimum of three (3) current and local references** for which you are providing same or similar products and services specified herein. Please indicate below the businesses for which you have provided such **during the past two (2) years:**

1. Company Name: _____

Address: _____

Phone #: _____ Fax #: _____

Contact Person: _____

Contract Period: From: _____ To: _____

Describe Services: _____

2. Company Name: _____

Address: _____

Phone #: _____ Fax #: _____

Contact Person: _____

Contract Period: From: _____ To: _____

Describe Services: _____

3. Company Name: _____

Address: _____

Phone #: _____ Fax #: _____

Contact Person: _____

Contract Period: From: _____ To: _____

Describe Services: _____

ATTACHMENT C

MCCCD EXTERNAL ENTITY DUE DILIGENCE QUESTIONNAIRE
SECURITY AND HOSTING STANDARDS AND PRACTICES

FOR COMPLETION BY EXTERNAL ENTITY WHEN APPLICABLE

Instructions for Completion of this Questionnaire:
This questionnaire must be completed if the product or service that MCCCD is being asked to adopt involves data and information that is not exclusively stored at MCCCD. By completing this questionnaire, you are verifying that your responses are based on personal knowledge and that they are the result of your due diligence to provide accurate and comprehensive information about the matter at hand.

The following table lists various security and privacy-related reports for which we ask that you provide information. Please indicate YES or NO for each of the following report types to indicate whether your organization has been the subject of an audit by an independent organization which evaluates and provides an opinion on the existence and effectiveness of information security controls.

Report Type 1: Department of Defense Certification and Accreditation	
Report Type 2: Federal Information Security Management Act (FISMA) Audit	
Report Type 3: Statement on Standards for Attestation Engagements (SSAE) No. 16	
Report Type 4: Service Organizational Control (SOC) 1, SOC 2 or SOC 3 [Note: The SOC 3 report is generally available and does not require an NDA; however, if your organization can provide only the SOC 1 or SOC 2, MCCCD Legal is willing to sign an NDA prior to disclosure.]	
Report Type 5: Payment Card Industry Data Security Standard (PCI DSS) Audit	
Report Type 6: Health Insurance Portability and Accountability Act (HIPAA) Audit	
Report Type 7: Federal Risk and Authorization Management Program (FedRAMP) security compliance certification	
Report Type 8: Other Audit by an independent organization which evaluates and provides an opinion on the existence and effectiveness of your organization's information security controls	

If you answered "Yes" to one or more of the above report types, please provide evidence or attach a copy of the corresponding report(s) with your response. You do not need to respond to the remaining questions.

If you answered "No" to each of the above report types, please complete the remainder of the questionnaire and submit it and all related documentation with your response.

For each of the following questions, please provide a copy of your organization's policy or other documentation that addresses the particular item. Please provide as much detail as possible in your responses. Feel free to include links to websites where further explanations may be found.

[Insert Name of External Entity Completing this Questionnaire] will reference these documents in our answers:

[EMBED POLICIES, MANUALS, REPORTS AND RELATED DOCUMENTATION IN THIS TABLE]

2.0 Security Policies

2.1 Organizational Security

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Are the following teams and individuals involved in information security at external entity and are their roles and responsibilities clearly defined? a) Executive-level oversight committee b) Corporate information c) All lines of business (LoBs) d) Individual information security managers who are assigned by each LoB		
2.	Do external entity's information security policies and practices include in sufficient detail guiding principles for: a) Development? b) Executive approval? c) Implementation? d) Maintenance?		
3.	Do external entity's information security policies promote the practice of: a) Compartmentalization of information? b) Least privilege? c) Need-to-know? d) Segregation of duties?		
4.	Are the following individuals subject to external entity organizational security policies? a) All full-time and part-time employees? b) Temporary employees? c) Independent contractors[1] and subcontractors[2]?		

[1] The term "independent contractor(s)" means independent contractors retained by external entity and its subsidiaries that provide services for the benefit of the external entity and its subsidiaries.

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
Additional Comments:			

2.2 Asset Classification and Control

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy define the following information assets as protected data and promote adherence to minimum handling requirements by all external entity personnel? a) Personally Identifiable Education Records - Covered under Family Educational Rights and Privacy Act (FERPA) b) Personally Identifiable Financial Information (PIFI/spiffy) - Covered under Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) c) Payment Card Information (PCI/epic) - Covered under Payment Card Industry Data Security Standard (PCI DSS) d) Protected Health Information (PHI/phi) - Covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)		
2.	Does external entity policy require implementation of anti-virus and personal firewall software?		
3.	Does external entity policy strongly recommend use of a computer program to manage the distribution of updates and hotfixes to computers in a corporate environment?		
4.	Do external entity asset classification and control security policies apply to the following individuals? a) All full-time and part-time employees? b) Temporary employees? c) Independent external entities and		

[2] The term "subcontractor(s)" means subcontractors retained by external entity and its subsidiaries that assist in performing all or any part of the services which the external entity has undertaken to perform.

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	subcontractors?		
5.	Do external entity policies establish requirements for acceptable non-personal business-related use of external entity's: a) Corporate network? b) Computer systems? c) Telephony systems? d) Messaging technologies? e) Internet access? f) Reprographic systems? g) Other company resources?		
Additional Comments:			

2.3 Human Resource Security

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity have a code of ethical conduct that: a) Establishes high standards for ethics and business conduct? b) Applies to every level of the company? c) Applies to every location where external entity does business throughout the world? d) Applies to all full-time and part-time employees? e) Applies to temporary employees? d) Applies to independent contractors and subcontractors? e) Covers the topic of legal and regulatory compliance? f) Covers the topic of business conduct and relationships? g) Requires compliance-tracked training that occurs biennially (i.e., once every 2 years) in: a. Ethics? b. Business conduct? c. Confidential information handling?		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
Additional Comments:			

2.4 Physical and Environmental Security

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy establish corporate-level mandates for complying with the U.S.-European Union Safe Harbor Program's EU Data Protection Directive of 1998 on maintaining the privacy and integrity of personal data?		
2.	Does external entity policy establish mandates for frequently undergoing the second of three AICPA (American Institute of CPAs) Service Organization Controls audits (i.e., the "SOC 2" audit) to measure the following controls related to external entity's provision of IT and data center services: a) Security? b) Availability? c) Processing integrity (ensuring system accuracy, completion and authorization)? d) Confidentiality? e) Privacy?		
3.	Does external entity policy provide corporate-level mandates for log retention, review and analysis covering: a) Minimum log requirements? b) Responsibilities for the configuration and implementation of logging? c) Alert review? d) Problem management? e) Retention? f) Security and protection of logs? g) Compliance review?		
4.	Does external entity policy establish information erasure guidelines that cover: a) Data erasure from all types of electronic media? b) Cost-benefit analysis of physical destruction vs. post-sanitization recycling?		
Additional Comments:			

2.5 Access Control

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy describe logical access control requirements for all external entity systems, including: a) Authentication? b) Authorization? c) Access approval? d) Provisioning? e) Revocation for employees and other external entity-defined 'users' with access to external entity systems that are neither internet-facing nor publicly accessible?		
2.	Does external entity policy require use of strong password controls by external entity employees[3], independent contractors, subcontractors and temporary employees that include instructions on how to: a) Choose effective passwords? b) Protect passwords? c) Change and store passwords and PINs?		
Additional Comments:			

2.6 Business Continuity Management

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy establish requirements for the development, maintenance and testing of the following: a) Emergency response? b) Disaster recovery? c) Business continuity practices?		
Additional Comments:			

[3] The term "external entity employees" means full-time and part-time employees of external entity.

2.7 Compliance

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require appropriate treatment by external entity of the following information assets that reside on external entity, customer and/or third-party systems to which external entity may be provided access in connection with the provision of the services: a) Personally identifiable education records? b) PIFI/ePIFI? c) PCI/ePCI? d) PHI/ePHI?		
2.	Does external entity policy require timely and efficient reporting of and response to information security incidents?		
3.	Does external entity maintain a detailed incident response plan that: a) Defines roles and responsibilities? b) Establishes procedures detailing actions taken during the incident based on: a. Incident type (e.g., virus, hacker intrusion, data theft, system destruction)? b. Severity of threat to system or data? c. Status of incident (e.g., active, contained)?		
4.	Does external entity policy provide requirements for external entity employees, independent contractors, subcontractors and temporary employees to notify identified contacts internally in the event of suspected unauthorized access to: a) Customer data? b) Personally identifiable education records? c) PIFI/ePIFI? d) PCI/ePCI? e) PHI/ePHI?		
Additional Comments:			

3.0 Physical Security Safeguards

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Do external entity physical security standards restrict access to service locations to only the following: a) External entity employees? b) Independent contractors and subcontractors? c) Temporary employees? d) Authorized visitors?		
2.	Do external entity standards require that identification cards be issued to and worn while on the premises by the following individuals: a) External entity employees? b) Independent contractors and subcontractors? c) Temporary employees? d) Authorized visitors?		
3.	Do external entity standards require authorized visitors to adhere to the following guidelines when on the premises: a) Sign a visitor's register? b) Be escorted and/or observed? c) Enter into a written confidentiality agreement with external entity? d) Return external entity-issued identification cards upon departure?		
4.	Do external entity standards require external entity security to monitor: a) Possession of keys/access cards? b) Ability to access service locations?		
5.	Do external entity standards require: a) Keys/cards to be returned by staff leaving external entity's employment? b) Keys/cards to be deactivated upon termination? c) After-hours access to service		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	locations to be monitored and controlled by external entity security? d) All repairs and modifications to the physical security barriers and/or entry controls at service locations to be authorized by external entity security?		
Additional Comments:			

4.0 Network Security

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy employ intrusion prevention and detection systems within the external entity network to provide continuous surveillance: a) For intercepting and responding to security events? b) In real time as security events are identified? c) By using a network-based monitoring approach to detect attacks on open ports? d) By using signature detection to match patterns of environment settings and user activities against a database of known attacks? e) By updating the signature database as new releases become available for commercial distribution? f) For dispatching alerts to external entity's personnel who will review and respond to potential threats?		
2.	Does external entity policy require use on the external entity network of: a) Access control lists? b) Segmentation to separate customer data?		
3.	Do external entity standards require: a) Management and monitoring by external entity's IT department of all routers and firewall logs? b) Safeguarding of network devices		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	via centralized authentication? e) Auditing of network usage?		
4.	Do external entity standards require external entity to access the environments residing on customer's system over the Internet by using either of the following technologies: a) Encrypted network traffic via another industry standard Virtual Private Network (VPN) or equivalent technology? b) Technology permitted by customer's network administrator?		
Additional Comments:			

5.0 Data Management/Protection

5.1 Deletion of Environments

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require that upon termination of services or at customer's request, external entity will: a) Delete the environments located on external entity computers in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on external entity preventing it from deleting all or part of the environments? b) Archive environments on tape for six (6) months following termination of the services, unless otherwise specified in writing by customer or by judicial or regulatory order?		
Additional Comments:			

5.2 Reporting Security Incidents

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require that if the customer contract specifies that external entity is required to access a production environment to perform the services and/or to receive production data		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	into a development or test environment to perform the services, external entity will take the following additional measures: a) External entity will frequently evaluate and respond to incidents that create suspicions of unauthorized misappropriation of customer's data, and external entity security will be informed of such incidents and, depending upon the nature of the activity, will define escalation paths and response teams to address the incidents? b) If external entity determines that data in customer's environment(s) may be or has been subject to a legal determination that a security incident has occurred (including by a external entity employee) or any other circumstance in which customer is required to provide a notification under applicable law, external entity will, unless otherwise required by law, report within 24 hours such misappropriation in writing to customer's privacy officer?		
2.	Does external entity policy require that external entity personnel be instructed in addressing incidents where handling of data has been misappropriated, including prompt and reasonable reporting and escalation procedures?		
Additional Comments:			

5.3 Disclosure of Data

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy prohibit external entity from disclosing data located on external entity, customer and/or third-party systems to which external entity may be provided access in connection with the provision of the services, including text and images, except in accordance with customer's contract, customer's written instructions, or to the extent required by law?		
2.	Does external entity policy require that external entity use diligent efforts to		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	inform customer, to the extent permitted by law, of any request for such disclosure before disclosure is made?		
Additional Comments:			

6.0 Access Control

6.1 Account Provisioning and Passwords

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require external entity to maintain the following standards for provisioning access to and creating passwords for the environments that are in the control of external entity: a) Access is provisioned on a need-to-know basis? b) Passwords conform to the strong password guidelines that include: a. Complexity? b. Expiration? c. Duplicity? d. Length? c) Passwords are neither written down nor stored on-line unencrypted in a reversible format? d) Passwords are treated as external entity confidential information? e) At customer's request, external entity will agree with customer on a schedule for periodic password changes? f) User IDs and passwords to customer's systems are not communicated to any other person without customer's prior written authorization?		
Additional Comments:			

6.2 General Access

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require in the event of employee terminations, deaths or		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	resignations, external entity will take actions to terminate network, telephony and physical access for such former employees?		
2.	Does external entity policy require that external entity security frequently review accounts of terminated employees to verify that access has been terminated and that stale accounts have been removed from external entity's network?		
Additional Comments:			

7.0 Additional External Entity Practices

7.1 Computer Virus Controls

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require external entity to maintain mechanisms within the external entity network for computers issued to external entity employees, independent contractors, subcontractors and temporary employees and with the following capabilities: a) Scans email sent both to and from any external entity recipient/sender for malicious code? b) Deletes email attachments that are infected with known malicious code prior to delivery?		
2.	Does external entity policy require all external entity employee, independent contractor, subcontractor and temporary employee laptops to be equipped with virus protection software?		
3.	Does external entity policy require external entity to maintain mechanisms that ensure: a) Virus definitions are frequently updated? b) Updated definitions are published and communicated to external entity employees, independent contractors, subcontractors and temporary employees? c) External entity employees, independent contractors, subcontractors and temporary		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	employees are able to automatically download new definitions and update virus protection software? d) Compliance reviews are frequently conducted by external entity?		
4.	Does external entity policy require all customer data stored on external entity employee, independent contractor, subcontractor and temporary employee laptops and removable media be encrypted?		
Additional Comments:			

7.2 Information Security Managers

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy establish the "Information Security Manager" role under which an advocate within external entity has the following responsibilities: a) Communicate information security awareness to external entity employees, independent contractors, subcontractors, temporary employees and management? b) Work effectively with external entity employees, independent contractors, subcontractors, temporary employees and management to help implement and comply with external entity's corporate security practices, policies and initiatives?		
Additional Comments:			

8.0 Human Resources Security

8.1 Personnel

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity code of ethical conduct require compliance with and acknowledgement of it by the following: a) External entity employees? b) Independent contractors? c) Subcontractors?		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	d) Temporary employees?		
2.	Does external entity code of ethical conduct stress reduction of the following risks: e) Human error? f) Theft? g) Fraud? h) Misuse of facilities?		
3.	Do external entity's efforts include: a) Personnel screening? b) Making personnel aware of security policies? c) Training employees to implement security policies?		
Additional Comments:			

8.2 Security Requirements

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require external entity employees, independent contractors, subcontractors and temporary employees to take the following measures to protect the security of the environments: a) Adhere to written confidentiality agreements? b) Comply with company policies concerning protection of confidential information? c) Store materials containing data securely and share those materials internally only for the purposes of providing the services? d) Dispose of paper copies of confidential materials and materials containing data in shredding bins designated for confidential information, and not in non-secure recycling bins or trashcans (if shredders are available at client site)?		
Additional Comments:			

8.3 Independent Contractors and Subcontractors

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy require that external entity enter into the following written agreements with each independent contractor and subcontractor: a) Confidentiality agreement? b) Services provider agreement that includes the external entity standards which require implementation of physical, technical and administrative safeguards consistent with external entity's obligations under the order and the *MCCCD External Entity Security and Hosting Standards and Practices* document? c) Network access agreement?		
2.	Does external entity policy establish that external entity is responsible for assuring that the independent contractors and subcontractors access, use and protect the security of the environments in a manner consistent with: a) The terms of the order? b) The *MCCCD External Entity Security and Hosting Standards and Practices* document?		
Additional Comments:			

8.4 Training

No.	Control Requirements	Yes/No ?	Comments/Compensating Controls
1.	Does external entity policy establish that all external entity employees, independent contractors, subcontractors and temporary employees complete online information protection awareness training that satisfies the following requirements: a) Conducted upon hiring and at least every two years thereafter? b) Instructs participants on their obligations under the various central external entity privacy and security policies? c) Instructs participants on data privacy principles and data handling practices that may apply to their jobs at external entity and are required by company policy, including those related to:		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	a. Notice? b. Consent? c. Use? d. Access? e. Integrity? f. Sharing? g. Retention? h. Security? i. Disposal?		
2.	Does external entity policy require that external entity: a) Perform periodic compliance reviews to determine if external entity employees, independent contractors, subcontractors and temporary employees have completed the online information protection awareness training course? b) Promptly notify and instruct external entity employees, independent contractors, subcontractors and temporary employees to complete training, if external entity determines they have not done so? c) Prepare and distribute written materials to promote awareness about security-related issues?		
Additional Comments:			

8.5 Enforcement

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
1.	Does external entity policy establish that: a) External entity conduct security reviews, assessments and audits frequently to confirm compliance with external entity information security policies, procedures and practices? b) External entity employees, independent contractors, subcontractors and temporary employees who fail to comply may be		

No.	Control Requirements	Yes/No?	Comments/Compensating Controls
	subject to disciplinary action, up to and including termination? c) External entity provide customer with a copy of the results of the security reviews, assessments, and audits within one week of either positive or negative results? d) If external entity materially fails a review, assessment and/or audit or is unable to execute an agreed-to remediation plan, customer may terminate the contract and any further payment obligation?		
Additional Comments:			

MCCCD EXTERNAL ENTITY SECURITY AND HOSTING PRACTICES AND STANDARDS

This document identifies the security practices that are required for External Entities performing information technology services for MCCCD.

I. Definitions

The term "Authorized Visitor" means visitors who are pre-approved by MCCCD to access the Environments.

The term "Continental United States" refers to all of the United States on the North American continent. The Continental United States includes 49 states, i.e., each of the 50 states exclusive of Hawaii.

The term "External Entity" means the entity that is responsible for performing information technology services for MCCCD. External Entity is also comprised of various teams and individuals involved in information security at External Entity, including the executive-level oversight committee, corporate information, all lines of business (LoBs) and individual information security managers ("ISMs") who are assigned by each LoB to represent the security leadership of each organization. Additionally, External Entity also includes any Subcontractor or third-party that External Entity deploys for the delivery of Services,

The term "Environment(s)" means MCCCD's technology environments to which External Entity is granted access in order to provide the services.

The term "Service Location(s)" means External Entity offices from which the Environments may be accessed.

The term "Service(s)" means the information technology service(s) described and set forth under a written contractual agreement between MCCCD and External Entity.

The term "Subcontractors" means subcontractors retained by External Entity and its subsidiaries that assist in performing the Services.

II. Security Policies

External Entity's corporate security policies must cover the management of security for both its internal operations as well as the Services External Entity provides to its customers, and apply to all External Entity employees, subcontractors and third-parties to External Entity, temporary employees, and individuals and legal persons that are involved in delivering services. These policies, which are aligned with the ISO/IEC 17799:2005 and ISO/IEC 27001:2005 standards, govern all areas of security applicable to the services.

Organizational Security

External Entity policy should describe the roles and responsibilities of various teams and individuals involved in information security at External Entity, including the executive-level oversight committee, corporate information, all lines of business (LoBs) and individual ISMs who are assigned by each LoB to represent the security leadership of each organization.

The policy should also describe the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at External Entity. This over-arching information security policy also describes governing principles such as 'need to know', least privilege, and segregation of duties.

- All individuals and legal persons who are involved in delivering Services are subject to External Entity security policies.

Asset Classification and Control

- External Entity policy should provide guidelines for all External Entity personnel regarding information classification schemes and minimum handling requirements associated with those classifications in an effort to ensure proper protection of External Entity and MCCCD information assets.

External Entity policy should require the implementation of anti-virus and personal firewall software and strongly recommends the use of Software Update Service (SUS) for Windows on desktop and laptop computers.

- External Entity policy should set requirements for use of the external entity corporate network, computer systems, telephony systems, messaging technologies, Internet access, and other company resources.

Human Resource Security

- External Entity should have a code of conduct that sets forth external entity's high standards for ethics and business conduct at every level of the company, and at every location where external entity does business throughout the world.
- The standards apply to employees, independent contractors, and temporary employees and cover the areas of legal and regulatory compliance and business conduct and relationships.
- Compliance-tracked training in ethics and business conduct and confidential information handling is required once every two years.

Physical and Environmental Security

- External Entity should have a policy that states corporate-level mandates for log retention, review, and analysis. Areas covered include minimum log requirements, responsibilities for the configuration and implementation of logging, alert review, problem management, retention, security and protection of logs, as well as compliance review.
- External Entity should have a policy that establishes guidelines for secure erasure of information, from all types of electronic and physical media, where use for current purposes is no longer needed and a decision has to be made regarding recycling or destruction. The policy is intended to protect external entity resources and information from security threats associated with the retrieval and recovery of information on electronic media.

Access Control

- External Entity should have a policy that describes logical access control requirements for all external entity systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other external entity-defined 'users' with access to external entity systems which are not Internet facing publicly accessible systems.
- External Entity should have a policy that requires protection of information assets by external entity employees, through the use of strong password controls where passwords are being used as a method of authentication.
- External Entity’s policy should describe the identity and access management method to define, allocate, adjust or remove an identity. The policy should address the characteristics of an identity, so as to ensure each identity is unique

Business Continuity Management

- External Entity should have a policy that addresses the requirements for the development, maintenance and testing of emergency response, disaster recovery, and business continuity practices to minimize the impact of business disruptive events on external entity’s internal business operations globally.
- External Entity has a Business Continuity Plan that addresses MCCCD’s business continuity requirements and this plan is tested at least once (1 time) every contract year

Compliance

- External Entity should have a policy that describes External Entity's treatment of data that resides on External Entity, MCCCD or third-party systems (including personally identifiable information or "PII") to which External Entity may be provided access in connection with the provision of the Services.
- External Entity must have a policy that requires reporting of and response to information security incidents in a timely and efficient manner. External Entity must also maintain a detailed incident response plan to provide specific guidance for personnel involved in or supporting incident response.
- External Entity must have a policy that provides requirements for External Entity employees to notify identified contacts internally, in the event of suspected unauthorized access to MCCCD data, PHI, PII and PCI.

III. Physical Security

Physical Security Safeguards: External Entity must maintain the following physical security standards, which are designed to prohibit unauthorized physical access at the Service Location(s).

- Physical access to Service Locations is limited to External Entity employees, Subcontractors and Authorized Visitors.
- External Entity employees, subcontractors and authorized visitors are issued identification cards that must be worn while on the premises.
- Authorized Visitors are required to sign a visitor's register, be escorted and/or observed when they are on the premises, and/or be bound by the terms of a confidentiality agreement with External Entity.
- External Entity security monitors the possession of keys/access cards and the ability to access Service Locations. Staff leaving External Entity's employment must return keys/cards and key/cards and all other access are deactivated upon termination.
- After-hours access to Service Locations is monitored and controlled by External Entity security.
- External Entity security authorizes all repairs and modifications to the physical security barriers or entry controls at Service Locations.

IV. Network Security

External Entity must take the following steps to secure access to the Environments:

- External Entity employs intrusion detection systems within the External Entity network to provide continuous surveillance for intercepting and responding to security events as they are identified. External Entity utilizes a network-based monitoring approach to detect attacks on open firewalls ports within External Entity's network. Events are analyzed using signature detection, which is a pattern matching of Environment settings and user activities against a database of known attacks. External Entity updates the signature database as new releases become available for commercial distribution. Alerts are forwarded to External Entity's IT department for review and response to potential threats.
- External Entity uses router rules, access control lists and segmentation on the External Entity network.
- External Entity's IT department manages and monitors all routers and firewall logs. Network devices are safeguarded via centralized authentication; usage is audited.
- When External Entity accesses the Environments residing on MCCCD's system over the Internet, it uses only (a) encrypted network traffic via industry standard Virtual Private Network (VPN) or equivalent technology, or (b) technology permitted by MCCCD's network administrator (e.g., direct dial-up or DSL if permitted on MCCCD's network). Unless otherwise specified in MCCCD's order, in (a) above, External Entity uses External Entity Continuous Connection Network (OCCN), which utilizes a persistent VPN tunnel and Cisco Software VPN Combination, for internet-based connections to the Environments.
- To the extent specified in MCCCD's order, External Entity may also use a desktop/laptop client based product when it accesses the Environments residing on MCCCD's system over the Internet. Examples include: Cisco Software VPN, Nortel Software VPN, Checkpoint Software VPN, Netscreen Software VPN, Point-To-Point Tunneling Protocol (PPTP), Neoteris Secure Sockets Layer (SSL) VPN, Aventail SSL VPN.
- External Entity shall ensure that all systems that contact MCCCD's network are controlled and managed from a virus protection perspective, to the extent that unmonitored or unwarranted systems (i.e. BYOD without External Entity Device Image) will be prohibited from connecting to MCCCD's network.

V. Data Management/Protection

Deletion of Environments: Upon termination of services or at MCCCD's request, External Entity will delete the Environments located on External Entity computers in a manner designed to ensure that they cannot reasonably be

accessed or read, unless there is a legal obligation imposed on External Entity preventing it from deleting all or part of the Environments. Unless otherwise specified in writing, External Entity will archive Environments on tape for six months following termination of the services. MCCCD shall be entitled to request a recovery of such backed-up Environments within the six months following termination.

Reporting Security Incidents: If the MCCCD contract specifies that External Entity is required to access a production Environment to perform the Services and/or to receive production data into a development or test Environment to perform the Services, External Entity will take the following additional measures:

- External Entity will promptly evaluate and respond to incidents that create suspicions of unauthorized misappropriation of MCCCD's data. External Entity security will be informed of such incidents and, depending upon the nature of the activity, will define escalation paths and response teams to address the incidents.
- If External Entity determines that data in MCCCD's Environments has been misappropriated (including by a External Entity employee), External Entity will report such misappropriation to MCCCD in writing.
- External Entity personnel are instructed in addressing incidents where handling of data has been misappropriated, including prompt and reasonable reporting and escalation procedures.

Disclosure of Data: External Entity will not disclose data located on External Entity systems, including text and images, except in accordance with MCCCD's contract, MCCCD's instructions, or to the extent required by law. External Entity will use diligent efforts to inform MCCCD, to the extent permitted by law, of any request for such disclosure before disclosure is made.

Crisis Management and Escalation Management: External Entity policy will provide a detailed plan to address an identified infection or high risk security breach (high risk event), Such policy will include the detailed activities that address escalation of the resolution of the high risk event, up to an executive level crisis management.

VI. Access Control

Account Provisioning and Passwords: External Entity must maintain the following standards for provisioning access to and creating passwords for the Environments that are in the control of External Entity:

- Access is provisioned on a need to know basis.
- Passwords conform to the strong password guidelines that include complexity, expiration, duplicity and length. Passwords will not be written down or stored on-line unencrypted.
- Passwords are treated as External Entity confidential information.
- At MCCCD's request, External Entity will agree with MCCCD on a schedule for periodic password changes.
- User IDs and passwords to MCCCD's systems are not communicated to any other person without MCCCD's prior authorization.

General Access: In the event of employee terminations, deaths or resignations, External Entity will take immediate actions to terminate network, telephony and physical access for such former employees. External Entity security will periodically review accounts of terminated employees to verify that access has been terminated and that stale

VII. Additional External Entity Practices

Computer Virus Controls*:* External Entity must maintain the following computer virus controls for computers issued to External Entity employees:

- External Entity maintains a mechanism within the External Entity network that scans all email sent both to and from any External Entity recipient for malicious code and deletes email attachments that are infected with known malicious code prior to delivery.
- External Entity requires all External Entity employee laptops or other devices that can access MCCCD's network to be loaded with virus protection software. External Entity maintains mechanisms to ensure that virus definitions are regularly updated, and that updated definitions are published and communicated to employees and other device users. These mechanisms also give employees and other device users the ability to automatically download new definitions and update virus protection software. From time to time, External Entity security will conduct compliance reviews to ensure employees and other device users have the virus software installed and up-to-date virus definitions on all desktops and laptops.

Information Security Managers: External Entity should have ISMs, who function as advocates within External Entity and carry the accountability to:

1. Ensure information security awareness to External Entity employees and management, and

2. Work collectively with that group to help implement and comply with External Entity's corporate security practices, policies and initiatives.

VIII. Human Resources Security

Personnel: All External Entity employees, independent contractors, and temporary employees must be required to abide by the External Entity code of ethics and by MCCCD rules, when visiting MCCCD sites. External Entity must place strong emphasis on reducing risks of human error, theft, fraud, and misuse of facilities. External Entity's efforts should include screening personnel, making personnel aware of security policies, and training employees to implement security policies. For example, employees are expected to have a clear understanding of password policies and policies concerning the handling of confidential information (in any form or shape).

Employee Security Requirements

External Entity employees must be required to take various measures to protect the security of the Environments. Employee obligations include written confidentiality agreements and compliance with company policies concerning protection of confidential information (e.g., External Entity code of conduct, acceptable use and information protection policies). Employees also are required to take the following measures to protect MCCCD's data:

- Store materials containing data securely and share those materials internally only for the purposes of providing the services.
- Dispose of paper copies of confidential materials and materials containing data in shredding bins designated for confidential information, and not in non-secure recycling bins or trashcans.

Subcontractors

- External Entity will obtain a written confidentiality agreement from each subcontractor before the subcontractor provides services. In addition, subcontractors that require access to MCCCD's Environments are required to sign a services provider agreement and a network access agreement. Included in the services provider agreement are the External Entity standards, which require the subcontractor to implement physical, technical and administrative safeguards consistent with External Entity's obligations under MCCCD's order and this document.
- External Entity is responsible for assuring that its subcontractors access, use, and protect the security of the Environments in a manner consistent with the terms of MCCCD's order and this document.

Employee Training

- All External Entity employees are required to complete information protection awareness training upon hiring and at least every two years thereafter. The course instructs employees on their obligations under the various central External Entity privacy and security policies. The course also trains employees on data privacy principles as well as data handling practices that may apply to their jobs at External Entity and are required by company policy, including those related to notice, consent, use, access, integrity, sharing, retention, security and disposal of data.
- External Entity performs periodic compliance reviews to determine if employees have completed the online data privacy awareness-training course. If External Entity determines that an employee has not completed this training, the employee will be promptly notified and instructed to complete such training as soon as practicable, and may be subject to disciplinary action.
- External Entity promotes awareness of, and educates employees about, issues relating to security. External Entity prepares and distributes to its employees notices and other written material on security.

Enforcement

- External Entity must conduct security reviews, assessments, and audits periodically to confirm compliance with External Entity information security policies, procedures and practices. Employees who fail to comply with information security policies, procedures and practices may be subject to disciplinary action, up to and including termination.
- MCCCD will be entitled to audit External Entity's Security Policies every year, once per year.

VII. Additional External Entity Practices

Computer Virus Controls*:* External Entity must maintain the following computer virus controls for computers issued to External Entity employees:

- External Entity maintains a mechanism within the External Entity network that scans all email sent both to and from any External Entity recipient for malicious code and deletes email attachments that are infected with known malicious code prior to delivery.
- External Entity requires all External Entity employee laptops and other devices used to connect to the MCCCD network to be loaded with virus protection software. External Entity maintains mechanisms to ensure that virus definitions are regularly updated on all devices, and that updated definitions are published and distributed to employee devices. From time to time, External Entity Global Information Security will conduct compliance reviews to ensure employees have the virus software installed and up-to-date virus definitions on all desktops and laptops.

CONTRACT TERMS

The following list provides examples of topics for security and privacy contractual terms that MCCCD External Entities may be asked to adopt:

Background Check and other Personnel Policies

Confidential Information

Cybersecurity Insurance

Dispute Resolution

Hosting Location

Maintenance and Incorporation of Privacy and Security Policies

Mitigation of Effect of Security Incident

Notification of Security Incident

Personnel Policies

Privacy Laws

Record and Data Retention, Ownership and Decommissioning

Termination for Breach