



Bharatiya Vidya  
**Bhavan**

# Bhavan's Vivekananda College

of Science, Humanities & Commerce  
Autonomous College - Affiliated to Osmania University  
Accredited with 'A' grade by NAAC  
Sainikpuri, Secunderabad - 500094



**NAAC RE-ACCREDITATION - 2ND CYCLE**

Criterion IV: -  
Infrastructure  
and Learning  
Resource

4.3.1  
IT Policy

*Submitted to*

**National Assessment and Accreditation Council**

## **IT Policy- Bhavan's Vivekananda College**

### **Internal Audit Committee**

- Principal - Chairman
- Head of Department, Department of Computer Science - Member
- Network Administrators - Members
- Two Teaching staff - Members
- Two Lab programmers - Members

### **Purpose of IT Policy**

- To maintain, secure, and ensure legal and appropriate use of Information Technology infrastructure established by the College on the campus.
- To establish College-wide strategies and responsibilities for protecting the information assets that are accessed created, managed, and/or controlled by the College.
- To work as a guide to stakeholders in the usage of the computing facilities of the College, including computer hardware, software, email, information resources, Intranet and Internet access facilities.
- To set direction and provide information about acceptable actions and prohibited actions or policy violations.

### **Scope of ITPolicy**

- College IT Policy applies to technology administered by the College centrally or by the individual departments, to information services provided by the college administration, or by the individual departments, or by individuals of the College community.
- This IT policy also applies to the resources administered by the departments such as Library, Computer Labs, Laboratories, and Administrative Offices of the College.
- Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the College IT policy.
- Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the College's information technology infrastructure, must comply with the Guidelines.
- IT Policy broadly focuses on the following areas:
  - IT Hardware Installation and Maintenance Guidelines
  - Software Installation and Licensing Guidelines
  - Network (Intranet & Internet) Use Guidelines
  - E-mail Account Use Guidelines
  - Website Hosting Guidelines
  - College Database Use Guidelines (Mastersoft ERP Solutions Pvt. Ltd.)
  - Role of Network/System Administrators

### **IT Hardware Installation and Maintenance Guidelines**

- IT Hardware Installation and Maintenance is performed by System Administrators.
- Faculty and the departments can submit IT Hardware requirements based on their academic requirements.
- Procurement of IT Hardware should be initiated based on the availability of stock and the requirements submitted by the departments.
- Stock Register should be updated immediately when IT Hardware is procured.
- IT Hardware Installation and maintenance services are provided only after receiving an approval from the concerned Head of the Department and the Principal.

- Maintenance of Computer Systems should be done periodically by System administrators and the same need to be recorded in the Maintenance Register.
- Movement of IT Hardware within the college or outside the college should be recorded in the Movement Register.
- The major e-waste such as written off instruments /equipment, CRTs, Printers, Computers, batteries etc., should be sold regularly.

#### **Software Installation and Licensing Guidelines**

- College IT policy allows authorized and open source software installation on the College computers. In case of any violation the College will hold the Department/Individual personally responsible.
- Open source software should be used in their systems wherever possible.
- Licensed software need to be installed in the systems.
- Antivirus Software needs to be procured and installed in the systems.
- Backup of Data should be taken periodically by the system administrators and stored in External Hard Disk or cloud outside resource.
- Software used for academic and administrative purposes should adhere to ISO standards.

#### **Network (Intranet & Internet) Use Guidelines**

- Any computer (PC/Server) that will be connected to the College network should have an IP address assigned by the System Administrators.
- An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the sameport.
- Change of the IP address of any computer by staff or student is strictly prohibited.
- Configuration of a network will be done by system administrators only.
- Individual departments/individuals connecting to the College network over the LAN may run server software only after bringing it to the knowledge of the System Administrators.
- Access to remote networks using the College's network connection must be in compliance with all policies and rules of those networks.
- Internet and Wi-Fi facilities should be used for academic and administrative purpose only.

#### **Email Account Use Guidelines**

- Every faculty member is provided with anE-mail.
- The E-mail facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- Using the E-mail facility for illegal/commercial purposes is a direct violation of the College's IT policy and may entail withdrawal of the facility.
- Faculty members should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
- Impersonating email account of others will be taken as a serious offence under the College IT security policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from violations of the College's email usage policy.

### **Website Hosting Guidelines**

- The College Website should be used to provide academic and administrative information for its stakeholders.
- Website Updation Committee is responsible for content updation and maintenance of the website.
- Maintain up-to-date pages. Proofread pages and test links before putting them on the Web, and regularly test and update links.
- The contents hosted on website should be correct and clear.
- The departments, and Associations of Teachers/Employees/Students may have an official Web page on the Website. Official Web pages must conform to the College Website Creation Guidelines.
- LMS (Learning Management System) can be linked to the website so that Faculty may post class materials (syllabi, course materials, resource materials, etc.) on the Web to facilitate e-Learning.
- Website Updating Committee needsto take proper measures in safe guarding the security of the data hosted.on the website.

### **College Database Use Guidelines**

- The databases are maintaine by the College administration with outsource management ( Mastersoft ERP Solutions Pvt. Ltd.). The Data should be backed up periodically in Cloud.
- Individuals or departments generate portions of data that constitute the College's database. They may have custodianship responsibilities for portions of that data.
- The College's data policies do not allow the distribution of data that is identifiable to a person outside the College.
- Data from the College's Database, including data collected by departments or individual faculty and staff, is for internal College purposes only.
- One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies the College makes information and data available based on those responsibilities/rights.
- Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the IQAC Office of the College.
- Requests for information from any courts, attorneys, etc. are handled by the Office of the College and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the IQAC Office of the College forresponse.
- At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes.
- Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to: Trying to break security of the Database servers.
- Certain violations of IT policy laid down by the College by any College member may even result in disciplinary action against the offender by the College authorities. If the matter involves illegal action, law enforcement agencies may become involved.

### **Responsibilities of Network/System Administrators**

- To Design College Network and perform Backbone operations.
- To follow Global Naming & IP Addressing conventions.
- To review the existing networking facilities, and need for possible expansion.
- Configuring and maintenance of Wireless Local Area Networks.
- To configure and maintain IT facilities provided in class rooms, Labs, Library, NSS, NCC, Sports and Committee Rooms etc.
- To receive and address complaints from users of the college network.
- To maintain servers in the server cabin.
- To look into the maintenance of Computer Hardware, Peripherals and Networking devices.
- To discourage installing any unauthorized software on the computer systems of the users. To strictly refrain from obliging the above said requests.

### **Protect personal and organization devices**

- Keep passwords of all devices protected.
- Choose and upgrade a comprehensive antivirus software.
- Ensure that devices are not left exposed or unattended.
- Install security updates of browsers and systems on a monthly basis, or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

### **E-waste Management**

- The Institution has undertaken a number of E-waste Management initiatives with the objective of creating an eco-friendly environment on the campus.
- E-Waste Management: Electronic goods are put to optimum use; minor repairs are set right by the Laboratory assistants and teaching staff; major repairs are handled by the Technical Assistant and are reused.
- The major e-waste such as written off instruments/equipment, CRTs, Printers, Computers are sold as per laid down policies.
- UPS Batteries are recharged / repaired / exchanged by the suppliers.
- Electronic gadgets, circuits, kits have been written off on regular basis and sold to buyers.
- All the miscellaneous e-waste such as CDs, batteries, fluorescent bulbs, PCBs and electronic items are collected from every department and office and delivered for safe disposal.
- The waste compact discs and other disposable non-hazardous items are used by students for decoration.
- Awareness programs have been undertaken in the institution, where the students are made aware of E-waste management techniques.

### **Vendors of IT support for the college**

- M/s Datatree Systems Pvt. Ltd, Hyderabad for college website [www.bhavansvc.ac.in](http://www.bhavansvc.ac.in) hosting and official emails of the college.
- M/s Mastersoft ERP Solutions Pvt. Ltd., Nagpur for college automation software, who have taken cloud support (role of security providers) from Microsoft Azure. Online payment Gateway has been implemented.

**College Examination Branch to maintain students' personal and exam marks data**

- The examination branch of the college maintains student personal data, and marks scored details in the branch local server.
- The data is protected with authenticated user access.
- While providing the results and marks details of students for semester end examinations, the software uses the authentication with Aadhaar card number to view the results/marks.
- The LAN link is provided to teaching staff to enter internal assessment marks with designated IP address, with proper login credentials.

**Secured WiFi access in the campus**

- The campus is provided with Wi-Fi access for staff only with proper secured credentials.
- The students are provided with internet access in the Library and Computer Laboratories through LAN access with proper access credentials.
- The staff are provided with Wi-Fi and LAN access to take online classes on the campus.

9/11  
29/12

**AGREEMENT**

**FOR CCMS ERP USAGES**

**AND**

**DATA PROTECTION & HANDOVER**

This Agreement is signed on 1<sup>st</sup> of December, 2018 between M/s MasterSoft ERP Solutions Pvt. Ltd. Nagpur, 1456-A, New Nandanvan, Nagpur-440024, India (hereinafter called the Supplier or Supplier) and BHAVAN'S VIVEKANANDA COLLEGE OF SCIENCE, HUMANITIES & COMMERCE SAINIKPURI, SECUNDERABAD(hereinafter called Purchaser). The term Purchaser also includes all the Users of Purchaser who will use the ERP such as – Staff, Officers, Faculty, students – parents, Trust management members & staff etc.

This agreement is undertaken for implementation of procured modules of Cloud based ERP CCMS – Centralized Campus Management System (hereinafter called as CCMS ERP) which is developed, hosted & owned by SUPPLIER. This Agreement may be amended on mutual understanding only in writing signed by a duly authorized representative of both parties. The Offer by Supplier & PO by Purchaser are part of this Agreement. In the witness thereof, the parties hereby agree as follows.

- **Agreement Period** : This agreement shall be for the period of five years, which can be renewed thereafter by written consent of both the parties on mutually agreed revised terms.
- **A Standard ERP**: After due diligence, Purchaser has agreed for standard ERP of Supplier. Since it's a Cloud ERP wherein one single ERP is/will be used by multiple Purchasers of different nature, Client specific changes in ERP are not feasible. Supplier will summarize most essential requirements from various Purchasers & globally acceptable changes / requirements will be incorporated in ERP periodically & will be automatically available to all the Purchasers. However these changes in ERP will be minimum & will be released normally four times in a year – quarterly.
- **Common ERP Upgrades**: Supplier may make suitable changes in product offerings & /or product platform due to changes in technology, Market Demands, Security concerns and the same will be available automatically to Purchaser. For optimization of ERP, rarely Supplier may discontinue some of the old / less used / redundant / out-of-date sub-modules / facilities. Supplier may remove/modify some of the facilities / menu options / processes based on Security reasons. Same will be applicable to Purchaser without any change in billing value.

---

Agreement For CCCMS ERP Usages And Data Protection & Handover Between –  
**BHAVAN'S VIVEKANANDA COLLEGE OF SCIENCE, HUMANITIES & COMMERCE**  
**SAINIKPURI, SECUNDERABAD & MasterSoft, Nagpur**



- **New paid facilities** : In case of any extra paid facility is offered by Supplier, Purchaser, if required, may procure the same with necessary payment.
- **Law** : Both the parties shall follow the law of the country & carry out the obligations /responsibilities as set out here under.
- **Official language** - Official language for oral and written communication is English.
- **Confidentiality** - Both Parties acknowledge and agree to maintain the confidentiality of Confidential Information (as hereafter defined) provided by the other Party (the "Disclosing Party") hereunder.
- **Non-solicitation** - Neither Party will, without the written consent of the other Party, employ directly or indirectly any person engaged or previously engaged by the other in any capacity in relation to the project, during the subsistence of this agreement and until a period of 30 months has expired after the termination or expiry of this agreement.
- **Purchaser Delays & Mistakes** : For any delays from Purchaser side, Purchaser will provide sufficient extra time to Supplier to complete its work. For all mistakes made by Purchaser's Users and noticed at later stage, correction at User end may not be possible. So, in such cases, Purchaser will communicate the same to the Supplier in writing via email for possible corrections. Supplier shall not be held liable for any delay or failure in its obligations, if such delay or failure has resulted from a delay or failure by Purchaser or third party to perform any of Purchaser obligations.
- **Termination for Material Breach** - Either Party may terminate this Agreement immediately by a Written notice to the other Party (i) in the event of a material breach by the other Party, by a written notice immediately, if the breach is not curable and by a written notice of 30 days, if the breach is curable and is not cured within the said notice period; or (ii) in the event of any proceedings in bankruptcy, insolvency or winding up filed by or against the other Party or for the appointment of an assignee or equivalent for the benefit of creditors or of a receiver or of any similar proceedings.
- **ERP IPR** - The ERP CCMS is developed by Supplier & it's Intellectual Property Rights – IPR are already owned by the company under India Copyright Act, 1957. The customizations / new process also will be IPR of Supplier, no Royalty is applicable to Purchaser. Supplier will use these customizations in its other products for other clients.
- **Scope of Service** : Scope of Service under this agreement is detailed in PO.
- **Additional Onsite Support** – beyond the scope of Supplier Offer & Purchaser PO - will be charged separately including Travel & Lodging.
- **Taxes** : Taxes shall always be extra & as per actual.
- **Other Expenses:** All Third party expenses (if any) shall always be extra.
- **Payment Terms** – Set up cost is to be given 100% advance along with PO by Purchaser and Student billing charges - yearly in advance – at the start of Academic session / After Admission.





- **Payment Delays** - In case of delay in payments - after 30 days from the due date, Access of ERP to all Users of the Purchaser would automatically discontinue without any notices. Same will be resumed after all the dues are cleared by Purchaser along with Cloud restoration Charges. To avoid various inconveniences due to Cloud disconnection, Purchaser needs to ensure On-time Payments. Non-availability of the Cloud Services to Purchaser Users due to Non-payment is an unavoidable process (Just like Electricity / water / telephone billing) and Purchaser needs to ensure 100% payment on-time to avoid such situation.
- **Price Escalation** – After one year, Actual escalation percentage will be discussed with Purchaser & decided as per Cloud revised rates.
- **No reduction PO value** - CCMS ERP charges once decided will not be reduced for the contract period for any reason. For any extra work which is beyond the scope of PO & Supplier agrees to provide the same or for extra modules, Supplier will quote / submit the bill. No reduction in billing is possible due to non utilization of ERP module by Purchaser team or for any other reasons whatsoever it may be..
- **Use of Supplier credentials** : Purchaser can use Supplier's logo name and all reports of ERP - in various reports / proposal submitted to UGC, NBA, NAAC, State Government, Central Government & other statutory committees, Educational conferences.....Supplier will be willing to help Purchaser for Academic improvement of Purchaser's Faculty & students on mutually agreeable terms. On demand, Supplier can sign MOU in the mutual benefit of Students-Purchaser & Supplier. Supplier will give Presentation of ERP in Purchaser's conferences – if requested by Purchaser. Supplier can give guest lecture to IT students of Purchaser.
- **Use of Purchaser credentials** – Similarly Purchaser agrees that Supplier shall have the right to list Purchaser's name & logo in its marketing material and for reference purposes. As a goodwill gesture, Purchaser, on request of supplier, will kindly talk to future probable Customers of Supplier and if required - will allow them to visit campus for ERP demo & discussions on mutually convenient dates. Purchaser will also issue written / video Testimonials to supplier on its request. Supplier can use sample data of Purchaser in its marketing presentations / communications / demos. No extra permission will be taken by Supplier in future.
- **Communication with students by Supplier**- Supplier will offer e-learning platform to the students of Purchaser's Campus. The standard version of e-learning platform will be free of cost to the Purchaser with defined storage space. Supplier in future may offer further new modules / concepts to the students as an initiative for betterment of students Education. Purchaser agrees that Supplier will communicate with students on email / mobile informing new features, modules, initiatives.....Purchaser hereby permits Supplier for such direct communication with students.



- **No access & decoding of ERP:** Copying / duplicating / decoding of the Supplier Application System is prohibited in all circumstances. Neither Purchaser nor any User is authorized to sell, license, sublicense, distribute, assign, transfer or distribute or timeshare the Supplier Application System or otherwise grant any right under this Use Terms to any third party (other than Authorized Users). Purchaser is not entitled to, and shall not make or permit others to reverse engineer, disassemble, de-compile, recreate, enhance or modify the Supplier Application System or any part thereof or to create enhancements to or derivative works of the Supplier Application System or any portions thereof.
- **No access to Database :** Cloud ERP & its Database structure is IPR of Supplier & same will be never available to Purchaser under any circumstances. Purchaser cannot write any programs using this data structure. No direct access to database can be provided to Purchaser. All the access will be thru ERP only.
- **On line Fees collection :** To avoid all cash transactions challenges & possible malpractices, Supplier strongly recommends Purchaser to accept all fees on-line & no cash transaction / minimum cash transactions.
- **Payment Gateway :** Supplier has integrated 2-3 standard Payment gateways after due diligence. Purchaser can choose one in consultation with Supplier. Supplier may give new Payment Gateway option to Purchaser based on changing market scenario. New payment gateway of Purchaser's choice can not be integrated by Supplier to ensure stability of its Cloud ERP. Purchaser has to choose an option from available with Supplier. Integrated Payment Gateway will allow all transactions type such as – Credit card, debit card, net banking.....
- **Supplier own PG:** Supplier will be launching its own payment gateway & will be made available to Purchaser in future. The services of Suppliers PG will be best.
- **No pre-printed stationary :** Supplier CCMS ERP does not support any pre-printed stationery formats. Most of the reports are available on A4 size plain copier paper of 60-100 GSM. To avoid misuse of pre-printed stationary, Supplier do not support Pre-printed Format for fees collection. Old Pre-printed stationary also can not be used.
- **New Client-specific Development:** All Standard Functionalities & Reports of procured modules will be available to Institute in this cost. Any New Functionalities & Reports required, if technically feasible, may be developed, and will be charged extra depending on the Scope. However this will be decided by Supplier.

Following Paragraphs define the Scope of Services & Responsibilities of Company, Responsibilities of Purchaser, General Terms & Conditions & Cloud understanding. Cloud understanding may change from time to time & detailed write-up of Cloud Understanding is defined by the Supplier on their website & is updated time to time and will be applicable to Purchaser from date of change. Purchaser shall study the same from

time to time and act accordingly.

## SCOPE & RESPONSIBILITIES OF THE SUPPLIER

- **ERP Enablement** : Supplier will enable procured modules of CCMS ERP system on Internet Servers (Cloud / VPS) at Supplier designated location(s). Supplier reserves the right to modify the Services Environment with minimum impact on the Services.
- **ERP commence Date:** The ERP Services may commence on the mutually agreeable dates – Maximum 45 days from the date of PO.
- **Permitted Use of Services:** Purchaser's use of Supplier Applications System will always be subject to the Licensing Conditions of the Supplier.
- **Training & Support** : The Supplier will configure & provide access to procured modules, demonstrate and train main Users & extend on-line service support to actual Users. The Supplier will give adequate training to the Users.
- **Privacy of Purchaser data:** Purchaser Data and processes privacy will be maintained by the Supplier. Only sample data may be used for demonstration to probable clients. No Data will be shared by Supplier with any third party for profit making.
- **Purchaser Data Inspection & reporting** : As a security measure, Supplier will continuously inspect, analyze the Purchaser data for any exceptions / challenges / data corruptions/ bugs / frauds / malpractices. Many reports will be generated & sent to Supplier on daily basis via email / post. Some reports / SMS will be auto generated.
- If errors are found, will either correct it or will inform to Purchaser authorities for their study & further probable action.
- **ERP Usages support** : Supplier will assist Purchaser Users in effective utilization of Cloud ERP modules.
- **No sharing of password** : Supplier team will **never** ask for User password from any User. Purchaser's User should never share password with Supplier team. Supplier team will never do any data entry / correction, processing work on behalf of Purchaser. Supplier can support Purchaser Users in doing their work at initial stages.
- **Common corrections:** In general, supplier will not modify finance data or exam marks or any other critical data of Purchaser without written / email consent from Purchaser. However some routine corrections / mistakes like updating : Common spelling mistakes in Master data, allotting common medium to many students, course level definition like - UG, PG...etc. which are essential for generation of many MIS & ADMS reports will be done by Company with due care. Theses corrections will be duly informed to Purchaser via e-mail.

## RESPONSIBILITIES OF PURCHASER

- **IT Infrastructure:** Purchaser will provide necessary hardware with healthy high speed internet to Purchaser's Users. Healthy – Continuous – good Bandwidth in-campus Internet Connection from multiple agencies is most essential need of Cloud based ERP.
- **ERP Co-coordinator:** Purchaser will provide one Co-coordinator / System Administrator for coordinating various activities with the Supplier for ERP implementation.
- **Training support :** Institute will ensure that the key personnel are available during Demonstrations & Training. Infrastructure for Training sessions will be organized by Institute and at a Centralized Location.
- **Division of Responsibility & Strict monitoring:** As far as possible, Purchaser should go for on-line fees collection mode to avoid any cash mis-handling. For security reasons, Purchaser will ensure that the reports printed by Counter/ Exam staff are always verified & certified by senior authorities. Fees transfer to Accounts module is always to be done by staff other than fees collection staff. A strict vigil is to be maintained on old cash collection receipts. Supplier's highest authorities will monitor fees & Exam transaction very carefully.
- **Guest House :** Free Hotel / Guest House Accommodation may kindly be provided to Supplier team by Purchaser for the onsite visit. If available
- **Data Entry :** Purchaser will be responsible for the Data Entry Work. The data from current session only can be entered. Data migration from existing system of Purchaser to Supplier ERP is not possible.
- **Data Ownership :** Purchaser will be the sole owner of the data uploaded and will be solely responsible for authenticity, accuracy, correctness & legality of the data.
- **Restricted Access:** Purchaser will limit the access of CCMS ERP to the Authorized Personnel. Each Authorized User will follow the security policies and rules as have been notified by Supplier. Purchaser will ensure that Services are for Purchaser use only and agrees that the Purchaser will not, in any way, commercially exploit the Services otherwise.
- **NO sharing of Password: In the interest of Purchaser data security & ERP security, there will be no un-authorized access to any unknown person / party. Pass-word shall never be shared by Purchaser Users with other Users, assistants, or with anyone including Supplier's staff.**
- **Information in advance :** Purchaser will inform all the important events & schedules, such as admission dates, exam dates, result dates well in advance via written communication so that Supplier's team can prepare & configure CCMS ERP accordingly.
- **Support Tickets:** Supplier assures best support to Purchaser Users. However in on-line environment, to avoid future issues, all Purchaser Users will raise all their

important support requirements thru on-line Ticketing System adopted by Supplier. Supplier ensures prompt time bound support against such tickets. In few cases, in interest of Purchaser, Supplier may request email / letter confirmation from Purchaser's higher authority. Purchaser should co-operate & same may be communicated to Supplier accordingly.

## Transaction Ownership

1. Purchaser will be solely responsible for all the transactions done thru authorised login. If Purchaser's User shares password to others or User itself enters wrong / fraud transactions, Purchaser will be solely responsible.
  2. Purchaser will be responsible for all activity occurring under its control and will abide by all applicable laws. The Purchaser will notify Supplier immediately of any unauthorized use of the Services or Services Environment. Purchaser undertakes that all Purchaser Data will not infringe the intellectual property rights of any third party. Supplier will also abide by all applicable laws of the land.
  3. Based on need / demand from various Educational Campuses, some special – compulsorily required facilities are provided by Supplier to Purchaser such as Receipt cancellation, Concession to students, backdated receipt entry, receipt for Scholarship.....At times these can be mis-used by Purchaser Users for their personal financial benefits. Supplier will be in no way responsible for any loss (Financial / goodwill) to Purchaser due to misusing of CCMS ERP by Purchaser's staff. A close watch needs to be kept by Purchaser's senior officers on such transactions...
  4. Purchaser agrees that Purchaser & its Users will be solely responsible for all the transactions done thru authorised logins. These transactions also includes all data entry & data modifications, Fees collection & Receipt cancellation, Admission cancellation, fees refund, modification of Fees demand, Back dated receipt entry & cancellation, On line Fees receipt cancellation, giving concessions, Master modifications/ deletion etc., It is necessary that Purchaser carefully gives privileges & access to the Users & keeps close monitoring on all the transactions - especially transactions related to fees & Marks of students.
  5. **Email alerts** : Purchaser Agrees that Purchaser will check the emails & take appropriate action (if required) send by Supplier on day to day basis.
- **ERP Settlement time** : Since this will be a totally Cloud based ERP involving multiple agencies such as Payment gateway company, Banks, Cloud company, there can be initial challenges to all the Users & Students. With its previous



experience, Supplier will attend the same & give appropriate solution to each issue. After few days, Users & student will get acquainted with Cloud ERP CCMS & understand the advantages of Cloud ERP. Lot of User support & understanding is required.

- **Download / print reports** : Purchaser can always download various reports / data (mostly in Excel format) on day to day basis as a safety measure. Purchaser must take data backup once a day for its safety.
- **Consultation with Supplier** : While procuring any hardware/software / on-line services such as Card printer, Biometric printer, new printers, Biometric machine, Card swap machines, Scanner.....; Purchaser must contact Supplier team for ensuring its feasibility of integration of the device with CCMS ERP. Normally Supplier do not supply such Hardware.
- **Check alerts** : Purchaser will check emails / alerts / SMS / What's-app / letter communication .....sent by CCMS cloud team. This will have very useful information / alerts about your college ERP data. Purchaser will take due action / cognizance of such communication.
- **E-Learning Contents** : Supplier is just an ERP Solution Provider. Actual usages is sole responsibility of Purchaser. While using CCMS ERP & its e-learning platform, Purchaser & Purchaser Users will ensure that contents uploaded do not violate any IPR / Copyright norms or Government laws. Purchaser & Purchaser Users are solely responsible for each & every uploaded contents - uploaded by them. Supplier will not have any legal obligations in this regard. Supplier will never validate the uploaded contents.

## **Payment Gateway & Other Third Party integration related responsibilities of Purchaser**

1. Third party interactions, certification and auditing, will be managed by Purchaser directly. Support needed by Supplier will be provided on case-to-case basis.
2. Supplier integrates most reputed & popular, User friendly Payment gateway. Best payment gateway will be recommended to Purchaser by Supplier team. Purchaser defined Payment Gateway integrations is not possible.
3. For Online fees collection necessary formalities / agreement shall be signed by Institute with Payment Gateway Company.
4. Payment gateway related issues are to be dealt with Payment Gateway Company directly. Payment gateway requires through understanding & Purchaser authorities would acquire the same gradually with the help of Payment Gateway Company staff.
5. The fees paid by students are collected by Payment Gateway Company and is directly transferred to the Purchaser's Bank

accounts – normally in two working days. Supplier only gets details of Transactions. Therefore, Queries related to Fees transaction will directly be transferred to the payment gateway provider and Supplier will have no role & responsibility in solving the transaction related queries.

6. Payment gateway activities are to be monitored by Purchaser staff on daily basis in consultation with Payment Gateway staff.

## GENERAL TERMS AND CONDITIONS

- **Browser support** : Application will support current versions as on date of popular browsers like Firefox, IE and Chrome with standard screen resolution of 1024 x 768 pixels.
- **Training module - Train the Trainer** : Supplier follows the train-the-trainer approach especially for faculty members & students who are large in number. A few Users of the solution (selected by Purchaser) will be provided training. Duration of this will be maximum up to 7 days at one common location. These Users are expected to train others on the solutions, including any ongoing / repeat training needs.
- **Usages of ERP:** Actual effective usages of the CCMS ERP modules will be the responsibility of the Purchaser. The Supplier can ensure necessary support to the Users of Purchaser.
- **Billing Cycle:** Yearly Advance payment
- **Contract period** : Five Years
- **Termination Clause:** The agreement can only be terminated with a 3 months written prior notice or payment in lieu thereof by the client. Nonpayment of dues to the extent of one month will attract discontinuation of cloud services by the Supplier and will be reinstated only upon regularization of payments so pending along with restoration charges. **Legal Jurisdiction** : Register office of city Supplier or Supplier city Courts
- **Effect of termination:** In the event of termination or expiry of this Agreement, (A) Purchaser will (i) forthwith cease to access and / or use any of SUPPLIER's Application Systems and Services Environment; (ii) return SUPPLIER any of SUPPLIER's confidential and proprietary information and material in its possession; and (iii) purchase Equipment at the then market value or the written down book value in SUPPLIER's books whichever is higher; and (B) SUPPLIER will (i) return to Purchaser all confidential and proprietary information of Purchaser;
- **Data sharing** : In case of termination, on release of all balance dues, on request from Purchaser, Supplier will share Purchaser data in Excel format.



- In case of discontinuation of Cloud ERP by Purchaser, Supplier will maintain the Purchaser data with itself, maximum for three months. Subsequently, Supplier will erase the data permanently.
- **Dispute Resolution** - As far as possible, for any dispute, Purchaser & Supplier's Management will settle such disputes at their own level. In case if this fails, Contract can be discontinued by either party by giving three months advance notice or money equivalent to three month billing of the Purchaser.
- **Force Majeure** : If either Party is unable to perform any of its obligations under this Agreement because of circumstances beyond the reasonable control of the Party, such as an act of God, fire, casualty, flood, war, terrorist act, failure of public utilities, Strike by employee, injunction or any act, exercise, labor or civic unrest, assertion or requirement of any governmental authority, epidemic, or destruction of IT facilities (a "Force Majeure Event"), the Party who has been so affected shall immediately give notice to the other Party and shall do everything reasonably practicable to resume performance. Upon receipt of such notice, all obligations under this Agreement shall be immediately suspended for the period of such Force Majeure Event. If the period of nonperformance exceeds sixty (60) days from the receipt of notice of the Force Majeure Event, the Party whose ability to perform has not been so affected may give written notice to terminate this Agreement. Termination clause will be as per PO.

## CLLOUD UNDERSTANDING

- **ERP availability** : ERP will be available to Users 24 hrs x 365 days. Normally User will get 98% uptime. So System will be available for nearly 8,600 hours in a year. In Manual / Client-Server based ERP, Purchaser has access to ERP maximum for 1250 hours. (250 working days in a year x 5 hours of working per day). So in all, seven times more time will be available on Cloud ERP to Purchaser Users.
- **Cloud Philosophy** : Cloud works on the philosophy, single ERP application with single database for all the Campuses with always latest single Cloud to all. So due to multiple Purchasers on same cloud, Purchaser specific customizations are not technically possible for any Purchaser. Cloud provides large configurations so that Cloud can be configured to match most of the User requirements with little cosmetic / Procedural compromises. So If CCMS Cloud is providing requirements with some cosmetic / Procedural limitations, User needs to accept it. No immediate customizations can be given to Campus. Certain important & must have requirements – which are technically feasible without affecting the ERP database structure - may be added by Supplier in





next update of Cloud – in the form of Configuration / Option. Till that time, User needs to use Cloud with certain alternative method proposed by Cloud expert team.

- **Cloud Implementation:** Cloud ERP is role based and very easy to use. Supplier will provide adequate training to Users. However it's a major application & success requires a lot of User Understanding + co-operation & management pursuance at initial stages. Most of the Purchasers are replacing their existing MIS with this new one. So Basic MIS structures of two MIS are different and User will need some time to adjust to new Cloud flow & methodology. Cloud can never be made same as Purchaser's old MIS. Purchaser User will never insist for Changes as per their old MIS. Such strong view by Purchaser User's will lead to either delays in implementations or at times in failures.
- **High speed internet in Campus:** High speed internet is must in Campus especially when students are accessing the Cloud MIS from Campus. Adequate Internet speed needs to be provided by Purchaser based on number of Users who may access Cloud MIS simultaneously from Campus. For un-interrupted internet connectivity, It is preferred that Campus has internet connections from multiple agencies with proper fire-wall so that users do not have access to unnecessary entertainment site where heavy internet may be used unnecessarily. Institute needs to make such arrangement. Purchaser may require extra internet at the time of admissions, examination when student will access Cloud regularly.
- **Cloud Software upgrade / Maintenance & downtime:** ERP will not be available or may be available at slow speed for short time during ERP patches uploading, backup, Cloud maintenance, Diagnostics analysis & security report generation – normally in late evening. Cloud Backup / Analysis time will be normally at midnight & system will be slow for an hour. In cloud technology, latest upgrades of procured modules are automatically available to all the Users with necessary documentation – all at no extra cost.

Normally all the **major ERP / MIS upgrades** will be uploaded in Cloud by Supplier after every three months, on Saturday afternoon & Sunday when Purchasers are not working with prior information on Cloud Server for all the Users - well in advance. However small patches will be uploaded regularly to meet urgent demands / security concerns. So Cloud will be off for Users for few minutes during patch uploading / few hours during major upgrade & testing.

However there can be a rare maintenance schedule (Scheduled / as well as breakdown) by Cloud company for Cloud Hardware, network, System software

or Malicious attacks. This will lead to non-availability of Cloud ERP to Users for few hours. All efforts will be taken to avoid any scheduled maintenance during Purchaser working hours.

- **Cloud Speed at User Computer:** The Supplier's Cloud service is of very high speed. However Speed of ERP at User Computer solely depends on configuration of User Computer / mobile, internet speed at that moment in his computer & Health of computer. For better speed of ERP, user needs to optimize his computer by making it virus free, removing cookies, deleting temporary file, deleting un-necessary software resident in RAM.
- **Data Security, Hacking, data Leakage Backup & Disaster Recovery:** Supplier will 100% ensure that there is no deliberate sell / sharing / leakage of Purchaser data to any third party. In case a Supplier employee is involved in such practices, strict action will be taken against him.

Best security methodologies are adopted by Supplier & they are continuously improved. Also multiple backup & recovery arrangements are in place. In case of any Disaster due to any reason (such malicious attack by Hackers / Virus / sabotage, Fire / Flood at Cloud premises, Earthquake/ damage due to Riots / strikes etc.); data may be lost / corrupted / leaked/compromised. Supplier's limited liability in this case will be immediate restoration of System & latest data from its backup & re-start the cloud services. Purchaser will co-operate with Supplier during this rarest of rare occasion, if occurs. If at all there is some data loss due to time gap between available backup & current status, Purchaser needs to re-enter the same. All over world, there is no solution of data loss / leakage / theft due to virus/ cybercrime & accidental disclosures and Supplier will not be liable for any Penalty or Criminal / civil cases for such events where there are no act of deliberate mis-conduct by Supplier.

However, Purchaser will also have a back-up provision by which Purchaser can download its data from Cloud as safety measure. To avoid data leakage / share from Purchaser end, Purchaser needs to ensure that only one person is responsible for such data backup operations & the person does not share the Password with anyone under any circumstances.

**SMS & Email Delivery:** With due diligence, Supplier has integrated a third party SMS Gateway in ERP which is common to all its Client & the same will be provided to Purchaser. SMS gateway services are governed by GOI TRAI norms / rules and hence Supplier will not be responsible for delays in SMS / Non receipt of SMS in few nos. As per TRAI / SMS company norms, SMS rates may get



# MasterSoft

ERP Solutions Pvt. Ltd.


*Accelerating education....*

changed in-between, without any notice. In such case, allotted SMS quantity to Purchaser may get reduced. No other – Client specific SMS Gateway will be integrated by Supplier.

**General : By using the CCMS Cloud ERP services in any manner it is deemed that Institute & its Users have accepted and are bound by the standard terms and conditions posted on CCMS Cloud ERP. The company Supplier ERP Solutions Pvt. reserves the right to modify/amend/add or deletes any of the terms and conditions mentioned on web site any time without any notice or information to the User. The User is requested to keep himself aware with any of the changes made in the terms and conditions and read & understand it thoroughly.**

IN WITNESS whereof the parties here to have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

Signed, Sealed and Delivered by the

 Mustak Ahmed Vice President - <b>MasterSoft ERP Solution Pvt. Ltd. Nagpur</b>	<b>BHAVAN'S VIVEKANANDA COLLEGE OF SCIENCE, HUMANITIES &amp; COMMERCE SAINIKPURI, SECUNDERABAD</b>
---	--

Date: 03/12/2020



# **Payment Card Industry (PCI) Data Security Standard**

---

## **Attestation of Compliance for Onsite Assessments – Service Providers**

**Version 3.2**

April 2016

## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

#### Part 1. Service Provider and Qualified Security Assessor Information

##### Part 1a. Service Provider Organization Information

Company Name:	Microsoft Cloud and Enterprise (C&E)	DBA (doing business as):	Not Applicable		
Contact Name:	Matt Rathbun	Title:	Chief Security Officer - Azure		
Telephone:	(425) 538-5404	E-mail:	Matt.Rathbun@microsoft.com		
Business Address:	One Microsoft Way	City:	Redmond		
State/Province:	WA	Country:	USA	Zip:	98052
URL:	https://www.azure.microsoft.com				

##### Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Divya Jeyachandran	Title:	Senior Manager, QSA		
Telephone:	303-554-6333	E-mail:	coalfiresubmission@coalfire.com		
Business Address:	11000 Westmoor Circle, Suite 450	City:	Westminster		
State/Province:	CO	Country:	USA	Zip:	80021
URL:	www.coalfire.com				

**Part 2. Executive Summary**

**Part 2a. Scope Verification**

**Services that were INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

Name of service(s) assessed:	Microsoft C&E: Datacenter Operations: Site services, Physical security services, Critical environments, Hardware destruction
------------------------------	--

Type of service(s) assessed:

<p><b>Hosting Provider:</b></p> <input type="checkbox"/> Applications / software <input checked="" type="checkbox"/> Hardware <input checked="" type="checkbox"/> Infrastructure / Network <input checked="" type="checkbox"/> Physical space (co-location) <input checked="" type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<p><b>Managed Services (specify):</b></p> <input checked="" type="checkbox"/> Systems security services <input checked="" type="checkbox"/> IT support <input checked="" type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<p><b>Payment Processing:</b></p> <input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

**Note:** These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

**Part 2a. Scope Verification** *(continued)*

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

Name of service(s) not assessed: Not Applicable

Type of service(s) not assessed:

<p><b>Hosting Provider:</b></p> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<p><b>Managed Services (specify):</b></p> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<p><b>Payment Processing:</b></p> <input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		

Others (specify):

Provide a brief explanation why any checked services were not included in the assessment:

Not Applicable

**Part 2b. Description of Payment Card Business**

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Microsoft C&E does not directly store, process or transmit cardholder data (CHD).
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	<p>Microsoft C&amp;E offers physical infrastructure hosting to their customers through Microsoft Azure. The Cloud and Enterprise (C&amp;E) division provides infrastructure and core services to other Microsoft business units. The C&amp;E Infrastructure Services offered are:</p> <ul style="list-style-type: none"> <li>• Datacenter Operations</li> <li>• Data Protection Services</li> </ul> <p>Microsoft Azure is a cloud service provider, offering hardware, infrastructure, and computing platforms for building, deploying, and managing applications and services. Microsoft Azure does this through a global network of Microsoft Corporation and third party managed datacenters. Microsoft Azure physical infrastructure is owned and managed by Microsoft C&amp;E. Microsoft Azure is a PCI DSS v3.2 validated Service Provider with AOC dated 3/4/2018.</p>

**Part 2c. Locations**

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

<b>Type of facility:</b>	<b>Number of facilities of this type</b>	<b>Location(s) of facility (city, country):</b>
Data Center	102	<p><b>North America</b></p> <ol style="list-style-type: none"> <li>1. Phoenix, AZ (PHX20)</li> <li>2. Santa Clara, CA (BY1/2/3/4/22)</li> <li>3. Des Moines, IA (DM1/2/3, DSM05)</li> <li>4. Chicago, IL (CH1/3, CHI20)</li> <li>5. San Antonio, TX (SN1/2/3/4/5/6)</li> <li>6. Ashburn, VA (BL2/3/5/7)</li> <li>7. Boydton, VA (BN1/3/4/6)</li> <li>8. Dallas, TX (DAL)</li> <li>9. Bristow, VA (BLU)</li> <li>10. Reston, VA (BL4/6/30)</li> <li>11. Tukwila, WA (TK5)</li> <li>12. Quincy, WA (CO1/2, MWH01)</li> <li>13. Cheyenne, WY (CYS01/04)</li> <li>14. San Jose, CA (SJC31)</li> <li>15. New York, NY (NYC)</li> <li>16. Stirling, VA (BL20)</li> <li>17. Toronto, Canada (YTO20, YTO01)</li> <li>18. Quebec City, Canada (YQB20)</li> </ol>



19. Mexico City, Mexico (MEX30)
20. Alpharetta, GA (ATL05)
21. Ogden, UT (SLC01)
22. Tulsa, OK (TUL04)

**Europe**

1. Vienna, Austria (VIE)
2. Vantaa, Finland (HEL01)
3. Amsterdam, Netherlands (AM1/2/3, AMS04/05/20)
4. Billingham, United Kingdom (MME20)
5. Chessington, United Kingdom (LON20/21)
6. Cardiff, United Kingdom (CWL20)
7. Dublin, Ireland (DB3/4/5, DUB06)
8. Paris, France (PAR02/21/22)
9. Marseille, France (MRS20)
10. Copenhagen, Denmark (CPH30)
11. Milan, Italy (MIL30)
12. Stockholm, Sweden (STO)
13. Bettemburg, Luxembourg (LUA)
14. Frankfurt, Germany (FRA20)

**Asia**

1. Hong Kong (HK1/2/20)
2. Mumbai, India (BOM01)
3. Dighi, India (PNQ01)
4. Ambattur, India (MAA01)
5. Osaka, Japan (OSA01/02)
6. Tokyo, Japan (KAW, TYO01/21/22)
7. Cyberjaya, Malaysia (KUL01)
8. Singapore (SG1/2/3, SIN20)
9. Busan, South Korea (PUS01, PUS20)
10. Seoul, South Korea (SEL20)

**South America**

1. Campinas, Brazil (CPQ01/02)
2. Fortaleza, Brazil (FOR01)
3. Rio de Janeiro, Brazil (RIO01)
4. Sao Paulo, Brazil (GRU)
5. Santiago, Chile (SCL01)
6. Humacao, Puerto Rico (PR1)

		<p><b>Australia</b></p> <ol style="list-style-type: none"> <li>1. Macquarie Park, Australia (SYD03)</li> <li>2. Melbourne, Australia (MEL01)</li> </ol>
--	--	---

**Part 2d. Payment Applications**

Does the organization use one or more Payment Applications?  Yes  No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

**Part 2e. Description of Environment**

Provide a **high-level** description of the environment covered by this assessment.

*For example:*

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

Microsoft C&E offers infrastructure services that enable customers to run enterprise and public applications on Microsoft C&E physical servers. Microsoft C&E does not directly transmit, process, or store any cardholder information; however, customers can implement an environment for storage, processing, or transmission of cardholder data using Microsoft C&E. Microsoft C&E cannot access customer data.

Does your business use network segmentation to affect the scope of your PCI DSS environment?  
*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*

Yes  No

**Part 2f. Third-Party Service Providers**

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?

Yes  No

If Yes:

Name of QIR Company: Not applicable

QIR Individual Name: Not applicable

Description of services provided by QIR: Not applicable

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?

Yes  No

**If Yes:**

<b>Name of service provider:</b>	<b>Description of services provided:</b>
Securitas	Physical Security, Camera monitoring at sites
Digital Trust Realty, Inc.	Physical Hosting Only
4Degrés	Physical Hosting Only
Global Switch	Physical Hosting Only

**Note:** Requirement 12.8 applies to all entities in this list.

## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

<b>Name of Service Assessed:</b>	Datacenter Operations: Site services, Physical security services, Critical environments, Hardware destruction			
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable:</b> Customer responsibility
Requirement 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable:</b> Customer responsibility
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable:</b> Customer responsibility
Requirement 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable:</b> Customer responsibility
Requirement 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable:</b> Customer responsibility
Requirement 6:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable:</b> Customer responsibility
Requirement 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable:</b> Customer responsibility
Requirement 8:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable:</b> Customer responsibility
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>9.6.2 Not Applicable:</b> Media is not sent outside of the storage facility. <b>9.6.3 Not Applicable:</b> Media is not sent outside of the storage facility. <b>9.9 Not Applicable:</b> No POI devices in scope <b>9.9.1 Not Applicable:</b> No POI devices in scope <b>9.9.2 Not Applicable:</b> No POI devices in scope <b>9.9.3 Not Applicable:</b> No POI devices in scope

Requirement 10:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable:</b> Customer responsibility
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>11.2 Not Applicable:</b> Customer Responsibility <b>11.2.1 Not Applicable:</b> Customer Responsibility <b>11.2.2 Not Applicable:</b> Customer Responsibility <b>11.2.3 Not Applicable:</b> Customer Responsibility <b>11.3 Not Applicable:</b> Customer Responsibility <b>11.3.1 Not Applicable:</b> Customer Responsibility <b>11.3.2 Not Applicable:</b> Customer Responsibility <b>11.3.3 Not Applicable:</b> Customer Responsibility <b>11.3.4 Not Applicable:</b> Customer Responsibility <b>11.3.4.1 Not Applicable:</b> Customer Responsibility <b>11.4 Not Applicable:</b> Customer Responsibility <b>11.5 Not Applicable:</b> Customer Responsibility <b>11.5.1 Not Applicable:</b> Customer Responsibility
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>12.3 Not Applicable:</b> Customer Responsibility <b>12.3.1 Not Applicable:</b> Customer Responsibility <b>12.3.2 Not Applicable:</b> Customer Responsibility <b>12.3.3 Not Applicable:</b> Customer Responsibility <b>12.3.4 Not Applicable:</b> Customer Responsibility <b>12.3.5 Not Applicable:</b> Customer Responsibility <b>12.3.6 Not Applicable:</b> Customer Responsibility <b>12.3.7 Not Applicable:</b> Customer Responsibility <b>12.3.8 Not Applicable:</b> Customer Responsibility <b>12.3.9 Not Applicable:</b> Customer Responsibility <b>12.3.10 Not Applicable:</b> Customer Responsibility <b>12.10 Not Applicable:</b> Customer Responsibility <b>12.10.1 Not Applicable:</b> Customer Responsibility <b>12.10.2 Not Applicable:</b> Customer Responsibility <b>12.10.3 Not Applicable:</b> Customer Responsibility <b>12.10.4 Not Applicable:</b> Customer Responsibility <b>12.10.5 Not Applicable:</b> Customer Responsibility <b>12.10.6 Not Applicable:</b> Customer Responsibility <b>12.11 Not Applicable:</b> Customer Responsibility <b>12.11.1 Not Applicable:</b> Customer Responsibility
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>A1.1 Not applicable:</b> Not a Shared Hosting Provider <b>A1.2 Not applicable:</b> Not a Shared Hosting Provider <b>A1.3 Not applicable:</b> Not a Shared Hosting Provider <b>A1.4 Not applicable:</b> Not a Shared Hosting Provider

Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>A2.1 Not applicable:</b> No POI devices in scope <b>A2.2 Not applicable:</b> No use of SSL/early TLS <b>A2.3 Not applicable:</b> No use of SSL/early TLS
--------------	--------------------------	--------------------------	-------------------------------------	---

## Section 2: Report on Compliance

---

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	6/30/2018	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 6/30/2018.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (**check one**):

<input checked="" type="checkbox"/>	<b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>Microsoft C&amp;E</i> has demonstrated full compliance with the PCI DSS.				
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby <i>Not Applicable</i> has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance: <i>Not Applicable</i></p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>				
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td>Not Applicable</td> <td>Not Applicable</td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met	Not Applicable	Not Applicable
Affected Requirement	Details of how legal constraint prevents requirement being met				
Not Applicable	Not Applicable				

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.



**Part 3a. Acknowledgement of Status** (continued)

- No evidence of full track data<sup>1</sup>, CAV2, CVC2, CID, or CVV2 data<sup>2</sup>, or PIN data<sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
- ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Not Applicable*

**Part 3b. Service Provider Attestation**

DocuSigned by:



43DC44914616444...

Signature of Service Provider Executive Officer ↑	Date: 6/28/2018
Service Provider Executive Officer Name: <b>Matt Rathbun</b>	Title: <b>Chief Security Officer - Azure</b>

**Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)**

If a QSA was involved or assisted with this assessment, describe the role performed:	Conducted PCI DSS v3.2 onsite assessment and documented compliance results in the Report on Compliance (ROC) and the associated Attestation of Compliance (AOC).
--	--



Signature of Duly Authorized Officer of QSA Company ↑	Date: 06/28/2018
Duly Authorized Officer Name: <b>Divya Jeyachandran</b>	QSA Company: <b>Coalfire Systems, Inc.</b>

**Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)**

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	<i>Not Applicable. No ISAs were involved with this assessment.</i>
---	--

<sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

### Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable

