1.

# Attachments

## Certificate of Compliance

VENDOR Organization Name

By indication of the authorized signature below, the VENDOR does hereby make certification and assurance of the VENDOR’S compliance with:

1. The laws of the State of Alabama;
2. Title VI of the Civil Rights Act of 1964;
3. The Equal Employment Opportunity Act and the regulations issued there under by the federal government;
4. The Americans with Disabilities Act of 1990 and the regulations issued there under by the federal government;
5. The condition that the submitted Proposal was independently arrived at, without collusion, under penalty of perjury;
6. The condition that no amount shall be paid directly or indirectly to an employee or official of the State of Alabama as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the VENDOR in connection with the procurement under this RFP;
7. The condition that if selected workmen's compensation insurance will be provided as required by the laws of Alabama;
8. The State of Alabama VENDOR Disclosure form;

and

1. Other terms and conditions as described in the Attachments as they apply.

VENDOR Name, Authorized Signature, Title, and Date

## VENDOR Exceptions

VENDOR Organization:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorized Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| Exception ID[[1]](#footnote-1) |
|  |
| Exception to[[2]](#footnote-2) |
|   |
| Scope of Exception |
|  |
| Ramifications for AMCC |
|  |
| Benefits and Disadvantages to be incurred by AMCC |
|  |

## Key Position Resume Sheet

This form must be used to respond to Section 4.7.2 – Key Positions. For each named individual a separate Key Position Resume Sheet must be submitted.

**VENDOR Organization:** **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Key Position: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Candidate:

Full Name: Last Name First Name MI

Address Street: City: State: Zip:

[ ]  U.S. Citizen [ ]  Non-U.S. Citizen Visa Status:

Status: [ ] Employee [ ] Self Employed [ ] Subcontractor ( Name: \_\_\_\_\_\_\_ )

 [ ] Other:

Education:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Mark highest level completed. | Some HS[ ]  | HS/GED[ ]  | Associate[ ]  | Bachelor[ ]  | Master[ ]  | Doctoral[ ]  |
| List most recent first, all secondary and post-secondary education (high school, GED, colleges, and universities) attended. Do **not** include copies of transcripts unless requested. Add additional rows if necessary |
| School Name | Degree/Major | Degree Earned | Year Received |
|  |  |  |  |
|  |  |  |  |

Work Experience:

Describe your work experience related specifically to the Request for Proposal to which you are responding. Please list most recent job first. **To add work experience, copy the format below and add additional sheets as needed**.

|  |
| --- |
| Work Experience #:  |
| Job Title:  |
| From | To  | Reason for Leaving: | Hours per week |
| Describe your duties and responsibilities as they relate to the Request for Proposal: |

References:

List 3 References below.

|  |
| --- |
| Reference 1 |
| Name | Title | Organization |
|  Address | Phone( ) -  | E-mail Address |

|  |
| --- |
| Reference 2 |
| Name | Title | Organization |
|  Address | Phone( ) -  | E-mail Address |

|  |
| --- |
| Reference 3 |
| Name | Title | Organization |
|  Address | Phone( ) -  | E-mail Address |

Candidate and VENDOR Certification

By submitting this data sheet to AMCC, the Candidate and VENDOR certify that, to the best of their knowledge and belief, all of the information on and attached to this data sheet is true, correct, complete, and made in good faith. The candidate further authorizes the release of all relevant prior employment, military service, academic/school, and criminal records. False or fraudulent information on or attached to this data sheet may be grounds for disqualifying a candidate or firing a candidate once work has begun. Any information provided to AMCC may be investigated.

By submitting this data sheet to AMCC, the Candidate and VENDOR certify that both parties understand the entire scope of requirements for this position as defined in the RFP and the Candidate agrees to be submitted for consideration exclusively by this VENDOR. Any candidate that is submitted by more than one VENDOR for a line item will be considered disqualified.

Candidate Data Sheets must be signed below by the VENDOR and the candidate.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Candidate Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorized Signature Date

## Sample Key Position Resume Sheet

**VENDOR Organization:** Auburn University Montgomery

**Key Position:**  Technical Team – Communications Manager

Candidate:

Full Name: Jackson Hewlett M

Address Street: 6760 Happy Lane Circle City: Oklahoma State: OK Zip: 54671

[x]  U.S. Citizen [ ]  Non-U.S. Citizen Visa Status:

Status: [x] Employee [ ] Self Employed [ ] Subcontractor (Name: \_\_) [ ] Other:

Education:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Mark highest level completed. | Some HS[ ]  | HS/GED[ ]  | Associate[ ]  | Bachelor[ ]  | Master[x]  | Doctoral[ ]  |

|  |
| --- |
| List most recent first, all secondary and post-secondary education (high school, GED, colleges, and universities) attended. Do **not** include copies of transcripts unless requested. Add additional rows if necessary |
| School Name | Degree/Major | Degree Earned | Year Received |
| Harvard University | Master Business Administration |  | 2001 |
| Yale University | Bachelor of Science in Information Technology |  | 2000 |
| Princeton University | Associate in Data Processing Technology |  | 1997 |

Work Experience:

Describe your work experience related specifically to the Request for Proposal to which you are responding. Please list most recent job first. **To add work experience, copy the format below and add additional sheets as needed**.

|  |
| --- |
| Work Experience #:  |
| Job Title: Sr. SQL Administrator |
| From02/2001 | To Present | Reason for Leaving: | Hours per week40 |
| Describe your duties and responsibilities as they relate to the Request for Proposal.Maintain and develop employee database, supply database, clientele databases, and administer programming for these databases, Keep all records up to date in hard copies and soft on a network. Keep general knowledge of network in order to coordinate employee computers. Keep clientele in a secure intranet database. |

|  |
| --- |
| Work Experience #:  |
| Job Title: Software Application Engineer |
| From03/1995 | To 01/2001 | Reason for Leaving:New Job Opportunity | Hours per week40 |
| Describe your duties and responsibilities as they relate to the Request for Proposal.Designs, develops, debugs, modifies, and tests software programs by using current programming languages, methodologies and technologies. Documents software development and/or test development by writing documents, reports, memos, change requests. Methods used are determined by approved procedures and standards Tracks software development effort by creating and maintaining records in the approved tracking management tool. Analyzes, evaluates, and verifies requirements, software and systems by using software engineering practices.  |

References:

List 3 References below.

|  |
| --- |
| Reference 1 |
| NameBob Thorton | TitleCEO | OrganizationBob Thornton Enterprise |
|  Address3245 Grey Hat Drive | Phone(123) 456 - 7589 | E-mail Addressbob@greyhat.com |

|  |
| --- |
| Reference 2 |
| NameHenry Ford | TitleCEO | OrganizationHumpfrey Corp. |
|  Address234 Humpfrey St. | Phone(123) 456 - 7589 | E-mail Addresshford@humpfrey.com |

|  |
| --- |
| Reference 3 |
| NameJack Daniels | TitleSoftware Director | OrganizationRed Brick Software Services |
|  Address987 Daniels Dr. | Phone(123) 456 - 7589 | E-mail Addressj@daniels.com |

Candidate and VENDOR Certification

By submitting this data sheet to AMCC, the Candidate and VENDOR certify that, to the best of their knowledge and belief, all of the information on and attached to this data sheet is true, correct, complete, and made in good faith. The candidate further authorizes the release of all relevant prior employment, military service, academic/school, and criminal records. False or fraudulent information on or attached to this data sheet may be grounds for disqualifying a candidate or firing a candidate once work has begun. Any information provided to AMCC may be investigated.

By submitting this data sheet to AMCC, the Candidate and VENDOR certify that both parties understand the entire scope of requirements for this position as defined in the RFP and the Candidate agrees to be submitted for consideration exclusively by this VENDOR. Any candidate that is submitted by more than one VENDOR for a line item will be considered disqualified.

Candidate Data Sheets must be signed below by the VENDOR.

[SIGNATURE]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Candidate Signature

[SIGNATURE]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorized VENDOR Signature

## STATE Security Risk Assessment

|  |
| --- |
| **STATE Third Party Vendor - Security Questionnaire** |
|  | **VENDOR Name:** | **Date:**  |
|  | **Designated Security Official Signature:**  | **Title:** |
|  | **Factors:** |

|  |  | **YES/NO** | **Comments** |
| --- | --- | --- | --- |
|  | **I. Security Policy**  |   |  |
|  | **A. Policy** |
| **1** | Is there a corporate information security policy in place? If yes, provide as an attachment. |   |   |
| **2** | Does the policy state what is and is not permissible as it pertains to sensitive company and customer information? |   |   |
| **3** | Does the policy identify what is classified as sensitive company and customer information? |   |   |
| **4** | Does the policy identify management and employee responsibilities including subcontractors? |   |   |
| **5** | Does the policy identify acceptable use of employee owned devices such as laptops, smart phones, and any other form of device capable of storing data? |   |   |
| **6** | Does the policy address requirements for change management procedures? |   |   |
| **7** | Does the policy address acceptable use of portable media to prevent malware from being introduced onto the corporate network and storage of confidential data? (e.g., thumb drives, CDRW, etc.) |   |   |
| **8** | Does the policy address onboarding and termination procedures for personnel? |   |   |
|  | **B. Procedures** |
| **1** | Are procedures and dedicated security personnel in place to implement the information security policy? |   |   |
| **2** | Are the procedures and standards evaluated to determine their level of impact to the business process? |   |   |
| **3** | Does the project management methodology uphold the security practices and goals of the Information Security Program?  |   |   |
|  | **C. Document Handling** |
| **1** | Is there a reasonable and usable information classification policy?  |   |   |
| **2** | Does the information classification policy address all enterprise information? |   |   |
| **3** | Is an information classification methodology in place to assist employees in identifying levels of information within the business unit? |   |   |
| **4** | Is there an information handling matrix that explains how specific information resources are to be handled? |   |   |
|  | **II. Corporate Practices**  |   |   |
|  | **A. Organizational Suitability** |   |   |
| **1** | Is there an executive level committee assigned to communicate and report on security risks to the organization? |   |   |
| **2** | Are employees able to perform their duties efficiently and effectively while following security procedures? |   |   |
| **3** | Does the information security program have its' own line item in the budget? |   |   |
| **4** | Does the security group have the authority to submit needed security policy changes throughout the enterprise? |   |   |
| **5** | Is an annual report on the level of information security compliance issued to management? If yes, please provide a copy. |   |   |
| **6** | Is there more than one person responsible for the implementation of the Information Security Program? |   |   |
|  | **B. Personnel Issues** |   |   |
| **1** | Are personnel required to have nationwide background check performed as part of the Information Security or Human Resources Policy? Please provide a copy of the VENDOR's Human Resources Policy if it is not part of the requested security policy in I-A-1. |   |   |
| **2** | Are contractors, subcontractors, and temporary staff subject to the same background check requirements? |   |   |
| **3** | Are employees and project managers aware of their responsibilities for protecting information resources via written policy? |   |   |
| **4** | Are technical employees formally trained to perform their tasks? |   |   |
| **5** | Are contract personnel subject to confidentiality agreements? |   |   |
| **6** | Are contract personnel subject to the same policies employees are? |   |   |
| **7** | Is access to confidential information by contract personnel monitored by the VENDOR? |   |   |
| **8** | Does the VENDOR's employment application ask a prospective employee if they have ever been convicted of a crime? If so, does the proposing firm employ individuals with felony and/or misdemeanor convictions? |   |   |
| **9** | Are prior employment verifications performed for initial employment? |   |   |
| **10** | Are there any current or pending litigation against staff, former staff, or contract staff regarding corporate espionage, identity theft, or any other areas regarding the security or privacy of confidential information? |   |   |
|  | **C. Training and Education** |   |   |
| **1** | Do employees receive security related training specific to their responsibilities? If yes, please attach a sample. |   |   |
| **2** | Are employees receiving both positive and negative feedback related to security on their performance evaluations? |   |   |
| **3** | Is security-related training provided periodically to reflect changes and new methods? |   |   |
| **4** | Are system administrators given additional security training specific to their jobs? |   |   |
|  | **D. Oversight and Auditing** |   |   |
| **1** | Are the security policies and procedures routinely tested? |   |   |
| **2** | Are exceptions to security policies and procedures justified and documented? |   |   |
| **3** | Are audit logs or other reporting mechanisms in place on all platforms? |   |   |
| **4** | When an employee is found to be non-compliant with security policies, is appropriate disciplinary action taken? |   |   |
| **5** | Are information security audits performed on an annual basis? |   |   |
| **6** | Are unscheduled/surprise audits performed? |   |   |
| **7** | Has someone been identified as responsible for reconciling audits? |   |   |
| **8** | Does either an internal or external auditor independently audit VENDOR’s operational controls on a periodic basis? |   |   |
| **9** | Is an independent review carried out in order to assess the effective implementation of security policies? |   |   |
| **10** | Can the VENDOR provide evidence of having gone through a recent audit of their organization’s operational policies, procedures, and operating effectiveness? Please provide copies of the most recent audits. |   |   |
| **11** | Has VENDOR experienced a security breach of corporate or customer data within the last 10 years? If yes, please provide additional information regarding the breach. |   |   |
| **12** | Is there is any concluded or pending litigation against the VENDOR or an employee related to a contract engagement or a security breach? |   |   |
| **13** | Does VENDOR have a change management committee? Does it meet on regularly scheduled intervals? |   |   |
|  | **E. Application Development and Management** |   |   |
| **1** | Has an application development methodology been implemented? |   |   |
| **2** | Are appropriate/key application users involved with developing and improving application methodology and implementation process? |   |   |
| **3** | Is pre-production testing performed in an isolated environment? |   |   |
| **4** | Have promotion to production procedures been implemented? |   |   |
| **5** | Are secure coding standards implemented and are they followed? |   |   |
| **6** | Are applications tested for security vulnerabilities prior to being released to production? Please provide a sample of the tests performed. |   |   |
| **7** | Is there a dedicated security team for testing applications for vulnerabilities? |   |   |
| **8** | Are there procedures in place for protecting source code developed by the VENDOR (physically and electronically)? |   |   |
| **9** | Is system access and security based on the concept of least possible privilege and need-to-know? |   |   |
| **10** | Does VENDOR perform source code reviews for each release? |   |   |
| **11** | Are backdoors prevented from being placed into application source code? |   |   |
|  | **III Physical Security**  |   |   |
|  | **A. Physical Security of Vendor Facilities** |   |   |
| **1** | Is access to corporate building(s) where company and customer information resides controlled? |   |   |
| **2** | Is access to computing facilities restricted to staff based on their job duties? |   |   |
| **3** | Is there an additional level of control for after-hours access? |   |   |
| **4** | Is there an audit log to identify the individual and the time of access that is monitored by a group other than Information Technology? |   |   |
| **5** | Are systems and other hardware adequately protected from theft? |   |   |
| **6** | Are procedures in place for proper disposal of confidential information? |   |   |
| **7** | Are proper fire suppression systems located in the facility? |   |   |
| **8** | Are computing facilities located more than 5 miles from a government facility or airport (high risk areas)? |   |   |
| **9** | Are the servers and facilities that house software documentation and programming logic located in a secure facility? |   |   |
| **10** | Is all confidential and restricted information marked as such and stored in a secure area (room, cabinet) with access restricted to authorized personnel only? |   |   |
| **11** | Does VENDOR allow employees to work remote or in a virtual environment? If yes, please provide documentation around controls for safeguarding computer systems and data in a virtual work environment. (Example: use of paper shredders to ensure confidential information is protected from disclosure) |   |   |
|  | **B. After-Hours Review** |   |   |
| **1** | Are areas containing sensitive information properly secured? |   |   |
| **2** | Are workstations secured after-hours such as screen lock out policy? |   |   |
| **3** | Are keys and access cards properly secured for open access areas? |   |   |
| **4** | Is confidential information properly secured from cleaning crews? |   |   |
| **5** | Are contract cleaning crews activities monitored? |   |   |
|  | **C. Incident Handling** |   |   |
| **1** | Has an Incident Response Team (IRT) been established? |   |   |
| **2** | Have employees been trained as to when the IRT should be notified? |   |   |
| **3** | Has the IRT been trained in evidence gathering and handling? |   |   |
| **4** | Are incident reports issued to appropriate management? |   |   |
| **5** | After an incident, are policies and procedures reviewed to determine if modifications need to be implemented? |   |   |
| **6** | Does the VENDOR have a process in place to notify IT security of a potential breach and/or other security problems to ensure proper notification and correction can be performed? |   |   |
|  | **D. Contingency Planning** |   |   |
| **1** | Has a Business Impact Analysis been conducted on all systems, applications, and platforms? |   |   |
| **2** | Is there a documented data center Disaster Recovery Plan (DRP) in place? |   |   |
| **3** | Are backup media passwords protected or encrypted? |   |   |
| **4** | Has the data center DRP been tested within the past 12 months? |   |   |
| **5** | Are system, application, and data backups sent to a secure off-site facility on a regular basis? |   |   |
| **6** | Are Service Level Agreements that identify processing requirements in place with all users and service providers? |   |   |
| **7** | Have departments, business units, groups, and other such entities implemented business continuity plans that supplement the data center DRP? |   |   |
| **8** | Have Emergency Response Procedures (ERP) been implemented? |   |   |
| **9** | Have ERPs been tested for effectiveness? |   |   |
|  | **IV. Business Impact Analysis, Disaster Recovery Plan** |   |   |
|  | **A. General Review** |   |   |
| **1** | Backup planning includes identification of all critical data, programs, documentation, and support items required performing essential task during recovery? |   |   |
| **2** | The BIA is reviewed and updated regularly with special attention to new technology, business changes, and migration of applications to alternative platforms? |   |   |
| **3** | Critical period timeframes have been identified for all applications and systems? |   |   |
| **4** | Senior management has reviewed and approved the prioritized list of critical applications? |   |   |
|  | **B. Disaster Recovery Plan (DRP)** |   |   |
| **1** | A corporate disaster recovery plan coordinator has been named and a mission statement identifying scope and responsibilities has been published? |   |   |
| **2** | A "worst-case" scenario DRP to recover normal operations within the prescribed timeframes has been implemented and tested? |   |   |
| **3** | Listing of current emergency telephone numbers for police, fire department, medical aid, and company officials are strategically located throughout the facility and at off-site locations? |   |   |
| **4** | The backup site is remote from hazards that endanger the main data center? |   |   |
| **5** | Contracts for outsourced activities have been amended to include service providers' responsibilities for DRP? |   |   |
| **6** | Lead times for communication lines and equipment, specialized devices, power hookups, construction, firewalls, computer configurations, and LAN implementation have been factored into the DRP? |   |   |
| **7** | Contingency arrangements are in place for hardware, software, communications, software, staff and supplies to meet DRP requirements? |   |   |
| **8** | Customer software solutions that are being developed and/or in production are backed up as part of the VENDOR's backup and recovery procedures? |   |   |
|  | **C. Testing** |   |   |
| **1** | Backup and recovery procedures are tested at least annually? |   |   |
| **2** | Training sessions are conducted for all relevant personnel on backup, recovery, and contingency operating procedures? |   |   |
| **3** | Appropriate user representatives have a particular role in creating and reviewing control reliability and backup provisions for relevant applications? |   |   |
| **4** | Appropriate user representatives participate in the DRP tests? |   |   |
| **5** | Insurance coverage for loss of hardware and business impact is in place? |   |   |
|  | **V. Technical Safeguards** |   |   |
|  | **A. Passwords** |   |   |
| **1** | Are host systems and servers as well as application servers secured with unique passwords? |   |   |
| **2** | Are default accounts de-activated? |   |   |
| **3** | Are temporary user accounts restricted and disabled within 24 hours? |   |   |
| **4** | Are the password management systems forcing personnel to change passwords every 90 days or less? |   |   |
| **5** | Are users of all company-provided network resources required to change the initial default password? |   |   |
| **6** | Are the passwords complex? Contain upper case, lower case, special character or number, and at least 8 characters long. |   |   |
| **7** | Do network and system administrators have adequate experience to implement security standards? |   |   |
| **8** | Are reports and logs pertaining to network users reviewed and reconciled on a regular basis? |   |   |
| **9** | Are permissions being set securely based on employee job responsibility? |   |   |
| **10** | Are administrators assigned a unique ID for access to critical systems? |   |   |
|  | **B. Infrastructure** |   |   |
| **1** | Is the network infrastructure audited on an annual basis? |   |   |
| **2** | Are network vulnerability assessments conducted on an annual basis? |   |   |
| **3** | Are changes/improvements made in a timely fashion following network vulnerability assessments? |   |   |
|  | **C. Firewalls** |   |   |
| **1** | Are protocols allowed to initiate connections from "outside" the firewall? |   |   |
| **2** | Has a risk analysis been conducted to determine if the protocols allowed maintain an acceptable level of risk? |   |   |
| **3** | Has the firewall been tested to determine if outside penetration is possible? |   |   |
| **4** | Are other products in place to augment the firewall level security? |   |   |
| **5** | Are the firewalls maintained and monitored 24/7? |   |   |
| **6** | Have services offered across the firewall been documented? |   |   |
| **7** | Has a Demilitarized Zone (DMZ) or Perimeter Network been implemented? |   |   |
| **8** | Has the firewall administrator been formally trained? |   |   |
| **9** | Is there more than one person administering the firewall? |   |   |
|  | **D. Data Communications** |   |   |
| **1** | Is there a remote access procedure in place? |   |   |
| **2** | Is there a current network diagram? |   |   |
| **3** | Are Access Control List (ACLs) maintained on a regular basis? |   |   |
| **4** | Is the network environment segmented from host where there is no business or IT requirement to communicate with other host? |   |   |
| **5** | Does the communication equipment log administrative access to the systems? |   |   |
| **6** | Is SNMP data collected from the data communication devices? |   |   |
| **7** | Is syslog data collected from the data communication devices? |   |   |
| **8** | Are there standard templates for configuring routers? |   |   |
| **9** | Are there standard templates for configuring switches? |   |   |
|  | **E. Databases** |   |   |
| **1** | Are default database passwords changed? |   |   |
| **2** | Are database administrators trained or certified? |   |   |
| **3** | Are database backups performed daily? |   |   |
|  | **F. Computing Platforms** |   |   |
| **1** | Are critical servers protected with appropriate access controls? |   |   |
| **2** | Does development staff have administrator rights on computers used for writing source code? |   |   |
| **3** | Is there a company image used for corporate PCs and laptops? |   |   |
| **4** | Does the company have an asset management system to track software installed? |   |   |
| **5** | Is there an anti-virus application installed on all PCs, laptops, and servers? |   |   |
| **6** | Does the anti-virus application automatically update computing assets 3 times or more per day? |   |   |
| **7** | Is there a URL filtering solution in place? |   |   |
| **8** | Are Internet facing servers protected with host based intrusion prevention? |   |   |
| **9** | Are employees including employees who may work remotely restricted to what can be installed on their computer systems? |   |   |
| **10** | Do any of the VENDOR's computer systems including storage reside on a cloud computing environment not owned by the VENDOR? |   |   |
|  | **G. Intrusion Prevention** |   |   |
| **1** | Is host based intrusion prevention software installed on all Internet facing servers and monitored 24/7/365? |   |   |
| **2** | Are network based intrusion prevention systems in-line and defending? |   |   |
| **3** | Is there a dedicated security staff monitoring security alerts 24/7/365? |   |   |
|  | **VI. Telecommunications Security** |   |   |
|  | **A. Policy** |   |   |
| **1** | Is there a published policy on the use of organizational telecommunications resources? |   |   |
| **2** | Have all employees been made aware of the telecommunications policy? |   |   |
| **3** | Employees authorized for Internet access are made aware of the organization's proprietary information and what they can discuss in open forums? |   |   |
| **4** | Are corporate devices such as iPhones or Android based phones centrally managed by the VENDOR to control rogue software installations and protect sensitive data? |   |   |
|  | **B. Standards** |   |   |
| **1** | Is there a threshold established to monitor and suspend repeated unsuccessful dial-in or remote access attempts? |   |   |
| **2** | Access to databases reachable via remote access or VPN have access controls in place to prevent unauthorized access? |   |   |
| **3** | Financial applications available via remote access or VPN have audit trails established to track access and transaction usage? |   |   |
| **4** | Are audit trails reviewed and corrective action taken on a regular basis? |   |   |
| **5** | When possible are ACL security programs used to control dial-in or remote access to a specific application? |   |   |
| **6** | Company proprietary data stored on portable computers are secured from unauthorized access? |   |   |
| **7** | Are corporate emails allowed to be sent from unique domains not used by the VENDOR such as Gmail or Microsoft Email? |   |   |
|  | **C. Practices** |   |   |
| **1** | Personnel independent of the operations staff and security administration review tamper-resistant logs and audit trails? |   |   |
| **2** | Employees are made aware of their responsibility to keep remote access codes secure from unauthorized access and usage? |   |   |
| **3** | Removal of portable computers from the corporate locations must be done through normal property removal procedures? |   |   |
| **4** | Employees are briefed on their responsibility to protect the property of the company when working away from the corporate environment? |   |   |

|  |
| --- |
| **VENDOR:** |
| **Authorized Signature:** | **Date:** |
|  | **Year 1****Cost** | **Year 2****Cost** | **Year 3****Cost** | **Year 4****Cost** | **Year 5** **Cost** |
| *List line item (e.g.: Project Management, Testing, Training, Maintenance, Hosting, Operations, etc.)* |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **Annual TOTAL Cost\*** |  |  |  |  |  |
| **TOTAL 5 Year Life-Cycle Cost\*** |  |  |  |  |  |

##  Cost Proposal Template

*\*Costs must be shown in U.S. dollars*

## Software Proposal Template

|  |
| --- |
| Complete Solution: License Model/Type must include brand, version number, unit pricing, licensing type, etc. Show numbers of licenses required under “QTY”. |
| VENDOR: |
| Date: |
| Authorized Signature: |
| Application Software |
| Software Module | QTY | License Model/Type & Price | Functionality Addressed |
|  |  |  |  |
| Third Party Software(Including reporting, conversion tools, data cleansing, data/application monitoring, etc.) |
| Brand Name & Version | QTY | License Model/Type & Price | Limitations or Additional Considerations |
|  |  |  |  |

## Customization Proposal Template

The proposed solution’s customization should be a best estimate based on information provided within this RFP. The pricing for the proposed solution’s customization will be reviewed and taken into consideration during contract negotiations.

|  |  |
| --- | --- |
| Functional Area | Pricing |
| Cultivation Tracking/Reporting |  |
| Processing Tracking/Reporting |  |
| Laboratory Testing Tracking/Reporting |  |
| Secure Transportation Tracking/Reporting |  |
| Dispensing Tracking/Reporting |  |
| Patient Dispensing  |  |
| Cannabis Product Availability Tracking/Reporting |  |
| Cannabis Destruction Tracking/Reporting |  |
| Cannabis Returns Tracking/Reporting |  |
| Production Statistics |  |
| Total: |  |

## Total Evaluated Price Template

|  |
| --- |
| Total Evaluated Price |
| Life Cycle (Total from Attachment 8.6) |  |
| Software (Total from Attachment 8.7) |  |
| Customization (Total from Attachment 8.8) |  |
| Total Evaluated Price |  |

## Hardware Proposal Template

|  |
| --- |
| Complete Solution: Description must include devices description or name, manufacturer, brand, model, part number, and /or other specifications such as compatible with specified software. **Note: AMCC will not be responsible for the purchase of the RFID tags or similar hardware.** |
| VENDOR: |
| Date: |
| Authorized Signature: |
| Component | Description | QTY | Business Rationale (Optional) |
|  |  |  |  |

## Functional Requirements

| **Requirement Number** | **Functional Requirements** | **Met without Modification** | **Met with Modification** | **Not Met** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| 1 | Allows for interface with other third-party inventory and tracking systems. To include but not limited to:* Licensee Seed-to-Sale System
* Patient/Caregiver Registry
* Business Licensing System
* Licensee Point of Sale Systems
 |  |  |  |  |
| 2 | Allows licensees to access or enter information into the statewide seed-to-sale tracking system directly and the licensee is not required to adopt and use a third-party inventory control and tracking system. |  |  |  |  |
| 3 | Allows for interface with other state agencies, and law enforcement personnel. |  |  |  |  |
| 4 | Provides the Commission and state agencies with access to information in the database that they are authorized to access. |  |  |  |  |
| 5 | Secures the confidentiality of information in the database by preventing access by a person who is not authorized to access the statewide seed-to-sale tracking system or is not authorized to access particular information.  |  |  |  |  |
| 6 | Ability to: configure and define user roles and access for commission, licensees, and other state agencies. |  |  |  |  |
| 7 | Provides user- and role-based security so that the system administrator can precisely control access permissions to solution features and transactions. |  |  |  |  |
| 8 | Provides the licensee with access to information in the tracking system that is necessary to verify that the licensee is carrying out all transactions authorized under the licensee's license. |  |  |  |  |
| 9 | Provides licensees with access to the information in the system that they are required to receive before a sale, transfer, transport, or other activity authorized under a license. |  |  |  |  |
| 10 | Assigns a globally unique, non-repeating identification number for every plant and inventory item recorded in the system. **Note: AMCC will not be responsible for the purchase of the RFID tags or similar hardware.** |  |  |  |  |
| 11 | Allows for interface with digital images, barcodes or QR Codes. |  |  |  |  |
| 12 | Tracks all cannabis plants, medical cannabis products, patient and caregiver purchase totals, waste, transfers, conversions, sales, and returns that are linked to unique identification numbers. |  |  |  |  |
| 13 | Tracks cannabis and medical cannabis sales and transfers among licensees. |  |  |  |  |
| 14 | Tracks cannabis and medical cannabis sales and transfers among facilities of the integrated facility licensees.  |  |  |  |  |
| 15 | Tracks lot and batch information throughout the entire chain of custody. |  |  |  |  |
| 16 | Tracks cannabis, product details, including weight and/or volume, at each stage: growing, processing, storage, laboratory testing, distribution, inventory, dispensing and destruction.  |  |  |  |  |
| 17 | Tracks all products, conversions, and derivatives throughout the entire chain of custody. |  |  |  |  |
| 18 | Tracks location of plants, any plant waste, and any plantings created from immature plants. |  |  |  |  |
| 19 | Tracks cannabis plant, batch, and product destruction. |  |  |  |  |
| 20 | Tracks products used in the cultivation of cannabis. To include but not limited to: * Pesticides
* Fungicides
* Growth Regulators
 |  |  |  |  |
| 21 | Tracks transportation of product; and allows for route plans and manifests to be entered into the system. |  |  |  |  |
| 22 | Reports and tracks loss, theft, or diversion of product containing cannabis.  |  |  |  |  |
| 23 | Tracks all inventory discrepancies. |  |  |  |  |
| 24 | Tracks reconciled inventory to include but not limited to:* Sales
* Transfers
* Waste Disposals
* Sampling
 |  |  |  |  |
| 25 | Retains an audit trail of modifications to records. To include instances where a licensee reports correction to existing data in the event of data entry error. |  |  |  |  |
| 26 | Allows the Commission to override information provided by licensees. |  |  |  |  |
| 27 | Receives testing results electronically from a state testing laboratory via a secured application program interface into the system and directly linking the testing results to each applicable source batch and sample. |  |  |  |  |
| 28 | Records all of the following attributes of any plant or product (but not limited to the following):* Potency
* Cannabinoid profile (including terpenes)
* Contaminants
* Microbes
* Mycotoxins
* Pesticides
* Solvent Residues
* Moisture Content
* Water Activity
* Heavy Metals
 |  |  |  |  |
| 29 | The ability to set threshold of accepted values (limits) for laboratory testing. |  |  |  |  |
| 30 | Provides information to cross-check that products received the required testing. |  |  |  |  |
| 31 | Identifies test results that may have been altered. |  |  |  |  |
| 32 | Tracks materials and *active and inactive* ingredients used in processing cannabis. |  |  |  |  |
| 33 | Performs complete batch recall tracking and identifies all the following details relating to the specific batch subject to the recall: a. Sold product. b. Product inventory that is finished and available for sale.c. Product that is in the process of transfer.d. Product being processed into another form.e. Postharvest raw product, such as product that is in the drying, trimming, or curing process. |  |  |  |  |
| 34 | Reports and tracks adverse patient responses or dose-related efficacy issues. |  |  |  |  |
| 35 | Produce reports electronically and for a given timeframe, including, but not limited to:* Cultivation Tracking/Reporting
* Processing Tracking/Reporting
* Laboratory Testing Tracking/Reporting
* Secure Transportation Tracking/Reporting
* Dispensing Tracking/Reporting
* Patient Dispensing
* Cannabis Product Availability Tracking/Reporting
* Cannabis Destruction Tracking/Reporting
* Cannabis Returns Tracking/Reporting
* Production Statistics
 |  |  |  |  |
| 36 | Ability to produce ad hoc reports on all data and metadata elements. |  |  |  |  |
| 37 | Provides analytics to the commission regarding key performance indicators such as the following: * Total daily sales
* Total cannabis plants in production
* Total cannabis plants destroyed
* Total inventory adjustments
 |  |  |  |  |
| 38 | Produce printable and downloadable chain of custody reports for plants, inventory, and products. |  |  |  |  |
| 39 | Tracks data from licensee to generate an inventory checklist on demand to resolve an immediate inventory discrepancy. |  |  |  |  |
| 40 | Retains record of date, time, amount, patient identification number, employee ID/name, and price of each sale or transfer of medical cannabis to a registered qualified patient or registered caregiver. |  |  |  |  |
| 41 | Provides information to cross-check that product sales are made to a registered qualified patient, or a registered caregiver on behalf of a registered qualified patient. |  |  |  |  |
| 42 | Reports and tracks all sales, sales tax, and refunds. |  |  |  |  |
| 43 | Scalable to account for developments including legislative changes, rulemaking provisions, and market demand.  |  |  |  |  |

1. Exceptions must be numbered in order as they occur within the RFP starting at 1. [↑](#footnote-ref-1)
2. VENDOR must fill this form for each exception separately. [↑](#footnote-ref-2)