

Contract for an IT Security  
and  
Staffing/Organization  
Assessment

State Center Community College District

October 21, 2013

CAMPUSWORKS

1767 Lakewood Ranch Blvd. #305  
Bradenton FL 34211  
T. 941.316.0308 | F. 941.954.2398

[www.campusWorksinc.com](http://www.campusWorksinc.com)

## Project Overview

Two senior CampusWorks professionals will conduct a 4.5-day on-campus assessment visit to include:

- A. IT Security Assessment:** This security assessment will determine the progress that has been made since the security issues were identified in the 2011/2012 CampusWorks assessment. The CampusWorks team will review the security reports completed by the District's insurance company, an external firm and internal information. The team will also conduct a review of current policy and procedures and conduct an onsite scan. An IT Security Assessment consists of review of state of organizational implementation of effective security controls safeguarding information, business processes, applications and infrastructure.
- B. IT Staff and Organization Assessment:** CampusWorks will provide an assessment of the current IT organizational structure, staff readiness and staffing allocation including assessment of IT positions essential to support the District's strategic objectives

The method for gathering information for the assessment will include a document review in advance of the onsite and the technical scans as described below. Individual and group interviews will be conducted with faculty, staff, students and standing committees during the onsite process.

The Chancellor will receive a written report detailing findings and recommendations resulting from the IT security and organization assessments. This report will include security findings and recommendations; a recommended organizational chart; staff strengths, weaknesses and opportunities for improvement; and recommended organizational plan to support the District's IT demands.

The complete presentation of findings, observations and recommendations will be presented 3 to 6 weeks after the assessment, pending availability of District staff.

## Exhibit A: Scope of Work/Methodology

### Information Technology Security Assessment

The IT Security Assessment consists of review of state of organizational implementation of effective security controls safeguarding information, business processes, applications and infrastructure. The methodology is aligned with the International Standards Organization/International Electrotechnical Commission standard ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security management and controls. An overview of the range of both topics explored as part of this engagement is outlined below:

1. IT GOVERNANCE COMMITMENTS AND RESPONSIBILITIES
2. INFORMATION SECURITY POLICIES, PROCEDURES & GUIDELINES
3. ENFORCEMENT
4. TRAINING AND EDUCATION
5. INFORMATION SECURITY PROGRAM
  - a. RISK ASSESSMENT & TREATMENT
    - i. *Assessing Security Risks*
    - ii. *Treating Security Risks*
  - b. ORGANIZATION OF INFORMATION SECURITY
    - i. *Information Security Infrastructure*
    - ii. *Security of Third Party Access*
    - iii. *Outsourcing*
  - c. ASSET MANAGEMENT
    - i. *Responsibility for Assets*
    - ii. *Classification Guidelines*
  - d. INFORMATION CLASSIFICATION
    - i. *Tier 1: Confidential*
    - ii. *Tier 2: Internal/Private*
    - iii. *Tier 3: Public*
  - e. IDENTITY AND ACCESS MANAGEMENT
    - i. *Identification*
    - ii. *Authentication*
    - iii. *Authorization*
    - iv. *Remote Access*
    - v. *Privileged Access*
    - vi. *Account Retention*
    - vii. *Segregation of Duties*
  - f. ACCESS CONTROL
    - i. *Business Requirement for Access Control*
    - ii. *User Access Management*
    - iii. *Password Policy*
    - iv. *User Responsibilities*
    - v. *Network Access Control*
    - vi. *Operating System Access Control*
    - vii. *Application and Information Access Control*
    - viii. *Monitoring System Access and Use*
    - ix. *Mobile Computing and Teleworking*
  - g. HUMAN RESOURCES SECURITY
    - i. *Prior to Employment*
    - ii. *During Employment*
    - iii. *Termination or Change of Employment*
  - h. COMMUNICATIONS AND OPERATIONS MANAGEMENT
    - i. *Operations Procedures and Responsibilities*
    - ii. *Third Party Service Delivery*
    - iii. *System Planning and Acceptance*
    - iv. *Virus Protection*

- v. *Encryption*
  - vi. *Network Security Management*
  - vii. *Backup and Recovery*
  - viii. *Media Handling*
  - ix. *Exchange of Information*
  - x. *Electronic Commerce Services*
  - xi. *Security Monitoring*
  - i. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE
    - i. *Security Requirements for Information Systems*
    - ii. *Security in Application Systems*
    - iii. *Cryptographic Controls*
    - iv. *Security of System Files*
    - v. *Security in Development and Support Processes*
    - vi. *Change Control*
    - vii. *Technical Vulnerability Management*
  - j. PHYSICAL AND ENVIRONMENTAL SECURITY
    - i. *Secure Areas*
    - ii. *Equipment Security*
    - iii. *Entry Controls*
    - iv. *Provisioning Processes*
    - v. *Alarms and Surveillance*
    - vi. *Visitors*
    - vii. *Computer Data and Media Disposal*
    - viii. *Equipment Disposal or Resale*
  - k. INFORMATION SECURITY INCIDENT MANAGEMENT
    - i. *Reporting Information Security Events and Weaknesses*
    - ii. *Incident Response*
    - iii. *Management of Information Security Incident and Improvements*
  - l. BUSINESS CONTINUITY MANAGEMENT
    - i. *Business Impact Analysis*
    - ii. *Disaster Recovery*
6. COMPLIANCE
- a. COMPLIANCE WITH LEGAL REQUIREMENTS, INCLUDING:
    - i. *Health Insurance Portability and Accountability Act (HIPAA)*
    - ii. *Family Education Rights and Privacy Act (FERPA)*
    - iii. *Health Information Technology for Economic and Clinical Health Act (HITECH)*
    - iv. *Gramm-Leach-Bliley Act for Disclosure of Nonpublic Personal Information (GLBA)*
    - v. *Red Flag Rules (RFR)*
    - vi. *Payment Card Industry Data Security Standards (PCI DSS)*
    - vii. *Digital Millennium Copyright Act (DMCA)*
    - viii. *Higher Education Opportunities act (HEOA)*
    - ix. *State Data Breach Notification Laws*
    - x. *Other State Statutes pertaining to Personal Information Protection*
  - b. COMPLIANCE WITH SECURITY POLICIES AND STANDARDS

- c. SYSTEM AUDIT CONSIDERATIONS
- 7. NON-INTRUSIVE VULNERABILITY SCANNING
  - a. OFF-HOUR SCANNING OF IDENTIFIED KEY SERVERS & SERVICES
  - b. CATEGORIZATION OF IDENTIFIED RISKS

### SCCCD Expectations

In advance of the assessment, organization will be asked to provide all pertinent documentation, including:

- All existing technology-related documented policies, procedures or guidelines (draft or published/public versions)
  - Including student handbook and employee security or technology compliance expectations or conditions of employment
- Any technology assessment performed internally or by outside engagement (infrastructure, security, process, etc.)
- Security audit finding (both final reports and questionnaires submitted as part of process)

The vulnerability scanning activity identified in section (7) requires direct physical connection and unfiltered access to all subnets/VLAN's hosting servers and services. Additional provision to access the network via all wireless networks (SSIDs) used by students, faculty, staff, and guests, as well as access from typical classroom and office locations.

### **IT Staffing and Organization Assessment**

CampusWorks will provide an assessment of the current IT organizational structure, staff readiness and staffing allocation including assessment of IT positions essential to support the District's strategic objectives. The staff assessment will determine:

- Staff readiness assessment in all departments to support the strategic and effective use of technology
  - Where is additional staffing essential? Where can staffing be optimized with new and additional training? Where can technology be used to maintain the current staffing levels, yet increase services provided? What is the ideal organizational structure to support SCCC?
  - Do clearly articulated business processes undergird the use of the technologies?
  - Is technology leveraged to optimize the use of human and financial resources?

- Recommendations to sustain or improve District performance against best practices for the strategic use of technology in community colleges, including:
  - Technology Leadership
  - Staffing
  - Program Prioritization

**Assessment Deliverable:**


- **Written Report:** The Chancellor will receive a written report detailing findings and recommendations resulting from the IT security and organization assessment. This report will include IT security findings and recommendations; a recommended organizational structure; staff strengths, weaknesses and opportunities for improvement; and recommended organizational plan to support the District’s IT demands.
- **Onsite Presentation:** The complete presentation of findings, observations and recommendations will be presented 3 to 6 weeks after the assessment, pending availability of District staff.

**Exhibit B: Investment Overview**

The fee for both components of this assessment consisting of 2.0 FTE is a fixed cost of \$44,500 and is inclusive of travel expenses. A deposit of \$22,250 is due upon execution of this agreement and the balance due upon delivery of the written report.

If you are in agreement with these terms, please email the signed document to [lmurphy@campusworksinc.com](mailto:lmurphy@campusworksinc.com) or fax to (941) 954-2398.

\_\_\_\_\_  
 Dr. Deborah Blue  
 Chancellor  
 State Center Community College District

  
 \_\_\_\_\_  
 Elizabeth A. Murphy  
 Chief Executive Officer  
 CampusWorks, Inc.

\_\_\_\_\_  
 Date

October 21, 2013  
 \_\_\_\_\_  
 Date

Institution Name: State Center Community College District  
 Address: 1525 East Weldon Avenue Fresno CA 93704

Business ID #: \_\_\_\_\_