FOOTHILL-DE ANZA COMMUNITY COLLEGE DISTRICT
REQUEST FOR PROPOSAL #1174

FOR

Consulting Services for Conducting an Information Security Audit

Submit proposals by October 10, 2008 to:
Foothill-De Anza Community College District
Purchasing Services Department
Building D-170
12345 El Monte Road
Los Altos Hills, CA  94022
Attn: Tom Lindstrom, Senior Buyer, Foothill -De Anza College District

KEY DATES
Submit all questions regarding this RFP by September 26, 2008
ATTN: Tom Lindstrom @ lindstromtom@fhda.edu
Proposals due October 10, 2008 by 4:00 p.m.
Recommendation for Award to Board of Trustees, estimated November 3, 2008
INTRODUCTION

Background: The District
The Foothill-De Anza Community College District (Foothill-De Anza) provides a dynamic learning environment that fosters excellence, opportunity and innovation in meeting the education needs of our diverse students and community. Located in the heart of Silicon Valley, Foothill-De Anza serves the communities of Cupertino, Los Altos, Los Altos Hills, Mountain View, Palo Alto, Stanford, Sunnyvale, and portions of San Jose.

For more than 40 years, Foothill-De Anza has demonstrated excellence and innovation in academic programs and student services. As one of the largest community college districts in the United States, Foothill-De Anza provides credit classes for about 44,000 students per quarter. The Colleges are members of the League of Innovation in the Community College, a national consortium of leading two-year institutions.

Background: Information Security
Educational Technology Services (the IT support organization within Foothill-De Anza) is seeking consulting services to assist in conducting an information security audit of key data management policies, processes and procedures. The proposed audit should help us define the unique requirements for establishing the effective security policies, processes, and procedures required to securely use and manage critical data. The audit, findings and recommendations will be focused on the critical financial, student information, human resources, and health data currently regulated by the Family Education Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPPA), Payment Card Information Data Security Standards (PCI DSS) and other applicable regulations. The deliverables will include recommendations for developing and implementing security policies, educational practices, guidelines and procedures by relevant District departments.

In addition, the audit should include recommendations for policies, education, practices, and technologies to assist Foothill-De Anza with control of user practices (such as peer-to-peer file transfers) on campuses that may constitute copyright infringement and may soon be regulated by legislation contained in US H.R. 4137, Sect 494.

Prospective consultants should have experience in conducting information security audits and developing information security plans for public higher education institutions (preferably in California) and a thorough knowledge of information security policies, practices, procedures, enforcement, security breaches and recovery, SCT Banner, FERPA, GLBA, HIPPA and PCI DSS. Prospective consultants should also be familiar and have experience with both higher education business process and process design in the areas of finance, student information, and human resources.

Background: Regulated Data
Definition of regulated data
1. For all individuals, an individual’s first and last name in combination with any of:
   - social security number
   - driver’s license number
2. For students: Personal information includes all personally identifiable information not included as directory information. This would be the student's name in conjunction with:
   - name of the student's parent(s) or other family members
   - address of the student's family
   - a personal identifier, such as a social security number or student number
   - race/ethnicity
   - gender
   - a list of personal characteristics
   - academic evaluations and grades
   - transcripts and other academic records
   - scores on tests required for new students
   - student's class schedule

3. For employees:
   - Employee ID number

SCOPE OF WORK

Objectives
The objective and approach of the proposed security audit must include:

1. Review and assess the current Foothill-De Anza policies, processes, and practices regarding the use, dissemination and administration of regulated data (financial, student information, human resource, health, and payment card information);
2. Present recommendations for mitigating security and compliance risks and improving the reviewed policies, processes, and practices in conjunction with the new Banner ERP system implementation;
3. Assess current practices and provide recommendations related to the control and management of possible campus software copyright infringement.
4. Audit the current policies and procedures, which grant access to security sensitive applications and recommend best practices to mitigate risks uncovered during the audit.

Scope
The proposed audit should cover all Foothill-De Anza data currently protected under the following regulations and standards:

- Family Education Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPPA)
- Payment Card Information Data Security Standards (PCI DSS)
- Pending legislations related to copyright materials protection
• Other applicable regulations

The proposed audit should include a review of the appropriate policies, processes, procedures and practices of the following Foothill-De Anza departments/functional units:
  • Educational Technology Services (ETS)
  • Finance
  • Financial Aid
  • Human Resources
  • Student Information/Registrar
  • Health Services (Foothill College)
  • Health Services (De Anza College)
  • Campus Bookstore
  • Athletics

The proposed audit should provide recommendations to mitigate the risks associated with the findings, including solutions to implement the Banner ERP system security infrastructure.

**Approach**

The proposed approach should include the following tasks:

• Work with District representatives to identify all campus systems, procedures and practices that utilize, store or transfer regulated data;
• Review the Appendix A (data flow) diagram and trace the data download, migration path to uncover any security flaws;
• Review formal and documented policies, processes and procedures that currently govern the use and administration of regulated data and the systems that store this data;
• Meet with appropriate District staff to review current processes and practices related to the use and administration of regulated data;
• Identify and document current risks;
• Develop and present recommendations for improving the District’s information security posture and compliance with regards to the use and administration of the regulated data under review;
• Meet and discuss with District management and ERP consultant to document the findings and solutions to the uncovered risks, make recommendations to incorporate the solutions for the Banner ERP security implementation.

**Deliverable**

The final deliverable for this project will be a report that includes recommendations for improving the District’s security policies, procedures, processes and practices related to the use and administration of regulated data. The proposal should also include a summary assessment of the current written or unwritten security policy and procedures in use within the District. These recommendations are to be prioritized and customized to the needs, constraints and opportunities of the District.
SUBMITTAL REQUIREMENTS

Introduction
The proposal shall include the following information:

• Name of company, address, telephone number of main office and any branch office that will be involved in any way with the project.
• Include the name, title, and address of the individual in your firm with the authority to negotiate contracts with the district.
• Summary of experience in the field of information security in higher education
• Summary experience of at least two (2) Banner ERP system security implementation
• A sample security audit report related to the similar engagement
• Description of services provided
• The scope of work
• Estimated timeline
• Hourly rate(s)
• Estimated total hours
• Description of expenses that would be charged to the District and how they would be calculated
• Total estimated cost including expenses
• At least three client references and contact information

GENERAL INFORMATION

Conflict of Interest.
These RFP procedures prohibit the practices which might result in unlawful activity including, but not limited to, rebates, kickbacks, or other unlawful considerations, and prohibit district employees from participating in the selection process when such employees have a relationship with a person or business entity seeking an agreement under this RFP that would create a conflict of interest.

Cost of Preparation.
The Foothill-De Anza Community College District is not liable for proposal preparation or submission expenses that may be incurred by the respondents.

Evidence of Insurance.
Include a copy of the proposer’s Certificate of Insurance. This may be marked confidential and included with the “original” (wet signature) proposal. The firm or organization shall be required to carry the following insurance:

• Comprehensive General Liability and Property Liability Insurance, with a minimum limit one million dollars ($1,000,000); aggregate amount $2,000,000.
• Comprehensive Automobile Liability Insurance, including owned, non-owned, and hired vehicles with minimum limit one million dollars ($1,000,000);
• Workers’ Compensation and Employers’ Liability, statutory limit;
In addition, the District at its own discretion may require a firm or organization to carry Professional Liability Insurance with minimum one million dollars ($1,000,000) per claim and two million ($2,000,000) per annual aggregate. Deductible not to exceed $25,000 each claim; and

All insurance must be issued by an admitted insurance carrier (licensed to do business in the State of California), carrying a rating of not less than A-VII in the most current A.M. Best’s Insurance Rating Guide - or otherwise acceptable to Owner.

QUESTIONS REGARDING THIS RFP

Questions regarding this Request for Proposals and further information should be directed to the District no later than 5:00 PM September 26, 2008. Submit information to the following individual:

Tom Lindstrom
lindstromtom@fhda.edu
(650) 949-6167

All questions will be responded to via an amendment. Amendments, if any, will be posted on BidNet and can be obtained free of charge by following the instructions at http://purchasing.fhda.edu/stories/storyReader$84.

PROPOSAL DUE DATE

All responses (1 original with 3 copies) to this Request for Proposals shall be submitted to:

Tom Lindstrom
Senior Buyer, Purchasing Services
Foothill – De Anza Community College District
12345 El Monte Road
Los Altos Hills, California 94022-4599

Faxed or e-mailed proposals will not be acceptable to the District. Sealed, hardcopy proposals will be received until 4:00 p.m. October 10, 2008. Any proposals received after the time specified in this notice shall be returned unopened.

EVALUATION CRITERIA

Submissions will be evaluated on the following criteria:

- Experience with information security and higher education: 20%
- Experience with Banner ERP system security: 20%
- Proposal content: 30%
- Total cost: 20%
- Reference information: 10%
Selected vendor will be required to enter into an Agreement for Services based upon the scope of work and deliverables described in this RFP. See attached sample of agreement.

ATTCH: Sample Agreement for Services
Appendix A: Foothill De Anza Data Flow Diagram

FRS, Process 1, 1099 Reporting

Diagram:
- Purchase Orders
- Invoices
- Check Requests
  - 1099 Tax IDs from W9 Form
  - FRS
  - 1099 Reports and Files
    - 1099 Files (text) created for District, Foundation, and History Center
    - 1099 Files Downloaded to Desktop (FTP)
      - 1099 files uploaded to IRS FIRE (web-based)
FRS, Process 2, Independent Contractor Reporting

FRS
Transfer Area

Extracts downloaded to IC folder on desktop. (FTP)

Extracts transmitted to EDD (web-based, e-file)

FRS

Bi-Weekly Data Extracts (new contractors)
**FRS, Process 3, ProCard**

Pro card is District issued credit card

1. ProCard Applications
2. FileMaker Cardholder Database
   - Fax
   - Web-Based (HTTP)

3. Bank of America
   - Monthly Card Charge Extract
   - Charges extract downloaded to desktop (FTP)
   - Charges data uploaded to FRS (FTP)

4. ProCards sent to District Office. Users contacted.

5. FRS
Check and Direct Deposit Runs (payroll accounts payable)

FRS

Check and Direct Deposit Extracts

VMS: CLERKS_AREA

Extracts transferred to workstation for check printing/direct deposit notices. (FTP)
FRS, Process 5, Bank of the West

Check and Direct Deposit Runs (payroll accounts payable)

FRS

Check and Direct Deposit Extracts

VMS: BWEST_AREA

Bank notified files are ready. (Fax)

Bank of the West
(Bank logs into captive account on VMS and retrieves files via analog transmission)
FRS, Process 6, Utilities
FRS, Process 7, E-Mail

FRS / VMS

Text extract for e-mail notifications (user name, e-mail address)

Mail Server
HRS, Process 1, HRS Transfer Area

1. HRS / VMS
2. HRS applications create data extracts.
3. VMS: HRS_TRANSFER
4. Extracts transferred to workstation, (FTP)
5. W2 Reporting (www.ssa.gov)
6. Staff Data Reporting (State Chancellor’s Office)
7. Employee Census File / Open Enrollment Data (FTP to Provider)
8. Other Agencies FTB, EDD, Credit Unions (Web or FTP Protocols)
HRS, Process 2, Liquid Office
Liquid office is a front end automated time reporting system
Check and Direct Deposit Runs (payroll accounts payable)

HRS

Check and Direct Deposit Extracts

VMS: CLERKS_AREA

Extracts transferred to workstation for check printing/direct deposit notices. (FTP)
HRS, Process 4, Bank of the West
Payroll processing direct deposit

Check and Direct Deposit Runs (payroll accounts payable)

HRS

Check and Direct Deposit Extracts

VMS: BWEST_AREA

Bank notified files are ready. (Fax)

Bank of the West
(Bank logs into captive account on VMS and retrieves files via analog transmission)
HRS, Process 5, Utilities
Download for desktop reporting from Oracle and other DBMS
HRS, Process 6, OID
ID download for portal database

LDIF files created for transfer to Oracle servers.

Portal Production  Portal Test
HRS, Process 7, PrimaMail
External W2 Payroll processing

HRS / VMS

Text extracts created.

Extracts are zipped, password-protected.

PrimaMail
Uses extract data to print and mail W2 forms.
SIS – Credential Inc.
Transcript processing

Transcripts

Transcript File, Enrollment Verification, Degree Check
SIS – EDI Smart

- DA Admin
- FH Admin
- E-Mail with PGP
- EDI Smart Texas Server
SIS – EtudesNG (Foothill College)
Distance learning student information processing
SIS – Medicat (Foothill College)
SIS – Moodle (De Anza College)
Distance Learning Student Information processing (De Anza College)
SIS – MIS

DA Admin

FH Admin

SIS and HRS Data (FTP Transfer)

Chancellor's Office
SIS – VMS Samba (De Anza College)