INTEGRATING SECURITY & ACCESSIBILITY IN IT PROCUREMENT

MARCH 4, 2020
Introduction

April Graham - Director, Contract, Procurement & Risk Management Services
Hsiawen Hull - Director, Technology Services
Santa Clarita Community College District

Background:

• College of the Canyons comprised of 2 campuses: Valencia & Canyon Country
• Approximately 17,000 FTES
• 5,492 Purchase Orders Processed in 2019
• 1,157 Contracts Processed in 2019
• 140 Software Products
Why Do We Care About Accessibility Now?

Timeline of Accessibility Events:

1998 – Identification of System-Wide Issues for Students with Disabilities
2017 – California State Audits Community College Technology Accessibility
2018 – Accessibility Standards and Resources
2019 – Website and Resource Certification
Why Do We Care About Accessibility Now?

ADA Complaints & Lawsuits:
- Domino’s Pizza
- Fox News Network
- Burger King
- CVS Pharmacy
- Target
- H&R Block
- Beyoncé
- Hobby Lobby
- Weight Watchers
- LACCD
- Harvard
- MIT
- Dept. of Homeland Security
- Small Business Administration
Why Do We Care About Accessibility Now?

• 1 out of 4 American adults have a disability that impacts major life activities including:
  o Mobility
  o Cognition
  o Hearing
  o Vision
  o Independent Living
  o Self-Care

• Internet is a place of public accommodation

• It’s a Purchasing law!
Why Do We Care About Security?

FERPA – Family Educational Rights and Privacy Act
◦ Protects the privacy of student education records
◦ Establish rights of students to inspect and review records
◦ Provides guidelines to the correction of records

HIPAA – Health Insurance Portability and Accountability Act
◦ Ensures patient access to records (Portability)
◦ Medicaid Integrity to prevent fraud/abuse
◦ Protect patient information
Why Do We Care About Security?

GLBA – Gramm-Leach-Bliley Act
- Established in 1999 establishing information sharing and security guidelines
- 2017 Educational institutions receiving Fed Financial aid enforcement

GDPR – General Data Protection Regulation
- Right to be forgotten(?)
- Data that may directly or indirectly identify an individual
- Provides regulations for how data used/stored
Why Do We Care About Security?

Unnamed College #1 Breached 2017 (Ransomware)
- Student Information System
- Network Shares
- Ransom Paid ($28k)

Unnamed College #2 Breached 2017
- Payroll Information

Unnamed College #3 2017
- PII without Security Controls
- Third-Party Vendor
Why Do We Care About Security?

Unnamed College #4 Breached 2018 (Suspected Ransomware)
- Student Information System
- Network Shares
- Email Systems
- End User Computers
- No Ransom Paid

Unnamed College #5 Breached 2019 (Ransomware)
- Email Systems
- Ransom Paid ($164k)
- Never Picked Up
- College was still encrypted as of 1/2020
Where Do We Start?

**Who, What, When, Where, Why and How**

1. Who will be using it?
2. How many employees?
3. How many students?
4. What is the product?
5. What does the product do?
6. What information will be stored/transmitted?
7. When will it be used?
8. Where will it be used?
9. How will it be used?
STEP 1: Identify Software

New

Obtain VPAT from Vendor

Obtain completed DSQ from Vendor

Submit for Evaluation

Existing

Obtain VPAT from Vendor

Obtain completed DSQ from Vendor

Any changes from previous VPAT & DSQ?

Yes

Submit for Evaluation

No

Purchasing Will Create Purchase Order
STEP 2:

Evaluate VPAT & DSQ

VPAT
- Cleared
- Conditionally Cleared
- Not Cleared
  - Submit RFC Form

DSQ
- Not Cleared
  - Submit RFC Form
- Cleared

Business Necessity?
- Yes
  - Submit RFC Form
- No
  - Purchase Not Allowed
Risk Evaluation:

Will this product be used by Students or the Public?

- YES
  - Cleared
    - Submit RFC Form
  - Conditionally Cleared
    - # of Staff Using Product?
      - 11 or more
        - Submit RFC Form
      - 10 or less
        - Submit RFC Form
  - Not Cleared
    - Business Necessity?
      - Yes
        - Purchase Not Allowed
      - No
        - Submit RFC Form

- NO
Risk Factors:

- **Low**
  - VPAT Clear
  - No PII
  - Low Student/Public Usage
  - Industry Standard
  - No Alternate Product Available
- **High**
  - VPAT Not Cleared
  - PII
  - Mid to High Student Use
  - Alternate Solutions are Available
  - Lack of Indemnification

---

**Contract Decision Tree**

- **Vendor Agrees to District’s Contract Terms**
  - Contract is Signed
  - Purchase Will Create Purchase Order

- **Vendor Does Not Agree to District’s Contract Terms**
  - High Risk
    - Contracts Dept. sends list of issues to Executive Cabinet Member (ECM)
  - Low Risk
    - Purchasing Will Create Purchase Order

- **ECM Weighs Risk Versus Business Need**
  - ECM Approves
    - Purchase Will Create Purchase Order
  - ECM Denies
    - Purchase Not Allowed

---

CISOA/3CBG 2018 CONFERENCE, ONTARIO, CA
The Complaint Department

508 Doesn’t Apply...Does It?

I Don’t Need to Complete the VPAT because it is VOLUNTARY.

We Don’t Need a VPAT because only Employees will be using the product.

- Who does it apply to?
- Instructional vs. Non-Instructional
- ADA, VPAT, WCAG and other fun acronyms
Trust, but Verify...

Somebody is Not Telling the Truth...

- Information provided on the VPAT does not match the product
  - 1-800-GET-HULL

- Information provided on DSQ does not match the items we know we are providing
  - 1-800-GET-MIKE
The Contract Gauntlet

Do I Really Need a Contract?

Why Do I Need a Contract?

We Never Needed a Contract Before!

Other Colleges Don’t Require a Contract

....and it’s a RUSH!
Standard Contract Clauses

Yes, we need a contract because:

- Term - Establishes a timeframe
- Payment - Defines amount and terms
- Scope of Work - Sets performance expectations
- Termination - Allow the District to terminate
- Indemnification - Mitigates or transfers risk
- Insurance – Financial back up
Software Contract Clauses

Other Important Contract Clauses To Consider:

- Definition of PII
- Security of Confidential Data
  - Ownership of Data
  - Prohibition on Unauthorized Use of Data
  - Remedies if Data Incident (Breach)
  - Maintenance of Security Measures (Written Information Security Program)
  - Reporting of Software Integrity Issues or Data Incident (Breach)
- Return of data upon expiration or termination
Software Contract Clauses

Other Important Contract Clauses To Consider

- Accessibility (verification of compliance, indemnification, contact for complaints)
- Service Availability
- Data Backup & Disaster Recovery
- PCI Compliance
- FERPA
- Limitation of Liability – STRIKE IT!!!
How Do We Get This Done?

1. Complete a Request For Contract (RFC) form.
   A. Describe the product and how it will be used.
   B. How many employees will be using the product?
   C. How many students will be using the product?
   D. Will personal information will be stored or transmitted?
   E. Please ask the vendor if there is an existing national, cooperative, or group purchasing contract that the District may purchase this software/product through?

2. Request a VPAT and DSQ from the Vendor.

3. Submit the completed forms to Contract Services.

4. IT will evaluate the DSQ and VPAT.

5. We’ll be in touch!
Best Practices

- Establish Policies and Procedures – CCLC BP/AP 3725
- Get the Details Up Front
- Collaborate!
- Maintain a Software Inventory
- Plan Ahead
- Ask Vendors for Updated VPATs and DSQs Twice per Year
- Promote Awareness