COLORADO STATE UNIVERSITY
PUEBLO

DEPARTMENT: INFORMATION TECHNOLOGY
AREA: INFORMATION SECURITY

CAE Memo: EVIDENCE OF SOUND CYBER SECURITY POSTURE AND SECURITY PLAN

To whom it may concern,

I hereby attest as the Colorado State University Pueblo (CSU Pueblo) Information Security Manager that CSU Pueblo provides its faculty, staff, and students with a sound cybersecurity plan.

I also attest to that the fact that CSU Pueblo has named me (**Mark D. Gonzales, Information Security Manager CSU Pueblo,** mark.gonzales@csupueblo.edu, cell: 719-549-2607) the dedicated on-campus official for all cybersecurity planning and implementation. Please reference Appendix H for my job description.

The following includes cybersecurity plan includes the following material, training, and policy.

2.1. Introduction to Data Security & Privacy
2.2. The Data Security Problem
2.3. What We Need to Protect
2.4. Threat Actors & Their Tactics
2.5. How We Can Protect Data
2.6. Responding & Reporting
2.7. Final Thoughts

1. Information Technology (IT) policies (ref. Appendix A).
2. Annual Data Security & Privacy training for all faculty, staff, and student employees via EverFi. This Data Security & Privacy training includes the following seven modules: (ref. Appendix B).
3. Annual Payment Card Industry Data Security Standard audit and training for all departments (includes faculty, staff, and student employees) handling credit card data. (Ref. Appendix C)
4. Monthly Information Security Working Group (ISWG) meetings focused on campus cybersecurity. Membership includes non-technical faculty, staff, and students. (Ref. Appendix D)
5. Monthly Information Technology Security Team (ITST) meetings focused on campus cybersecurity. Membership includes technical staff and IT student employees. (Ref. Appendix E)
6. Management of a campus Information Security (InfoSec) website under the IT department banner for all faculty, staff, students. This website focuses on cybersecurity, data security, and information security. (Ref. Appendix F)
7. The monthly publication of a InfoSec Newsletter for all faculty, staff, students. This is a one page newsletter of cybersecurity current threats and recommendations to keep campus and personal data secure. (Ref. Appendix G)

Mark D. Gonzales September 29, 2021

Mark D. Gonzales Information Security Manager, Colorado State University Pueblo Date

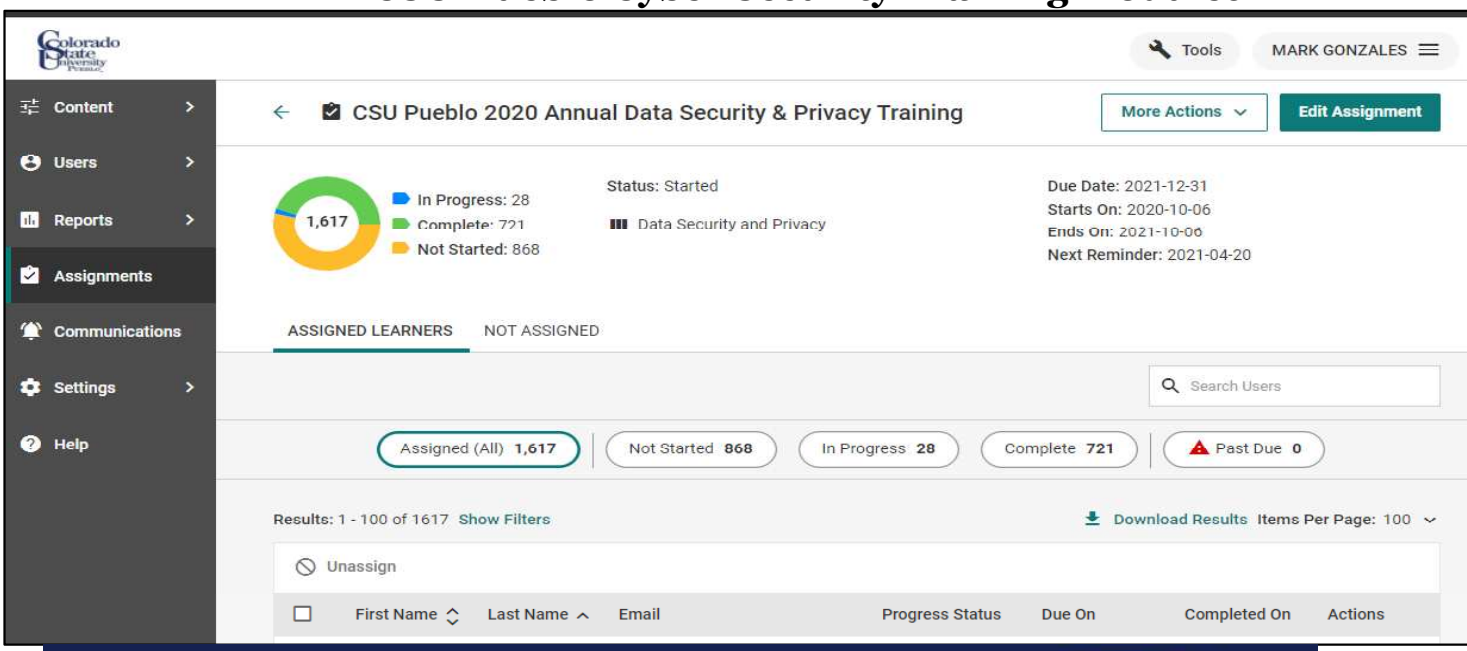
COLORADO STATE UNIVERSITY
PUEBLO

APPENDIX A

CSU PUEBLO IT POLICIES	
Title	Link
Acceptable Use Policy for Technology Resources	http://csu-pueblo-policies.colostate.edu/policy.aspx?id=27
Computer Crime Policy	http://csu-pueblo-policies.colostate.edu/policy.aspx?id=49
CSU-Pueblo Web Policy	http://csu-pueblo-policies.colostate.edu/policy.aspx?id=139
eAccount Policy	http://csu-pueblo-policies.colostate.edu/policy.aspx?id=48
Email and Electronic Mass Communications Policy	http://csu-pueblo-policies.colostate.edu/policy.aspx?id=15
Password Policy	http://csu-pueblo-policies.colostate.edu/policy.aspx?id=50
Server Policy	http://csu-pueblo-policies.colostate.edu/policy.aspx?id=51
Toll Free Number Policy	http://csu-pueblo-policies.colostate.edu/policy.aspx?id=52
Wireless Deployment Management Policy	http://csu-pueblo-policies.colostate.edu/policy.aspx?id=53

COLORADO STATE UNIVERSITY
PUEBLO

APPENDIX B-CSU-Pueblo Cyber Security Training Modules



COLORADO STATE UNIVERSITY
PUEBLO

APPENDIX C

Image 1: Blackboard Learning Management System

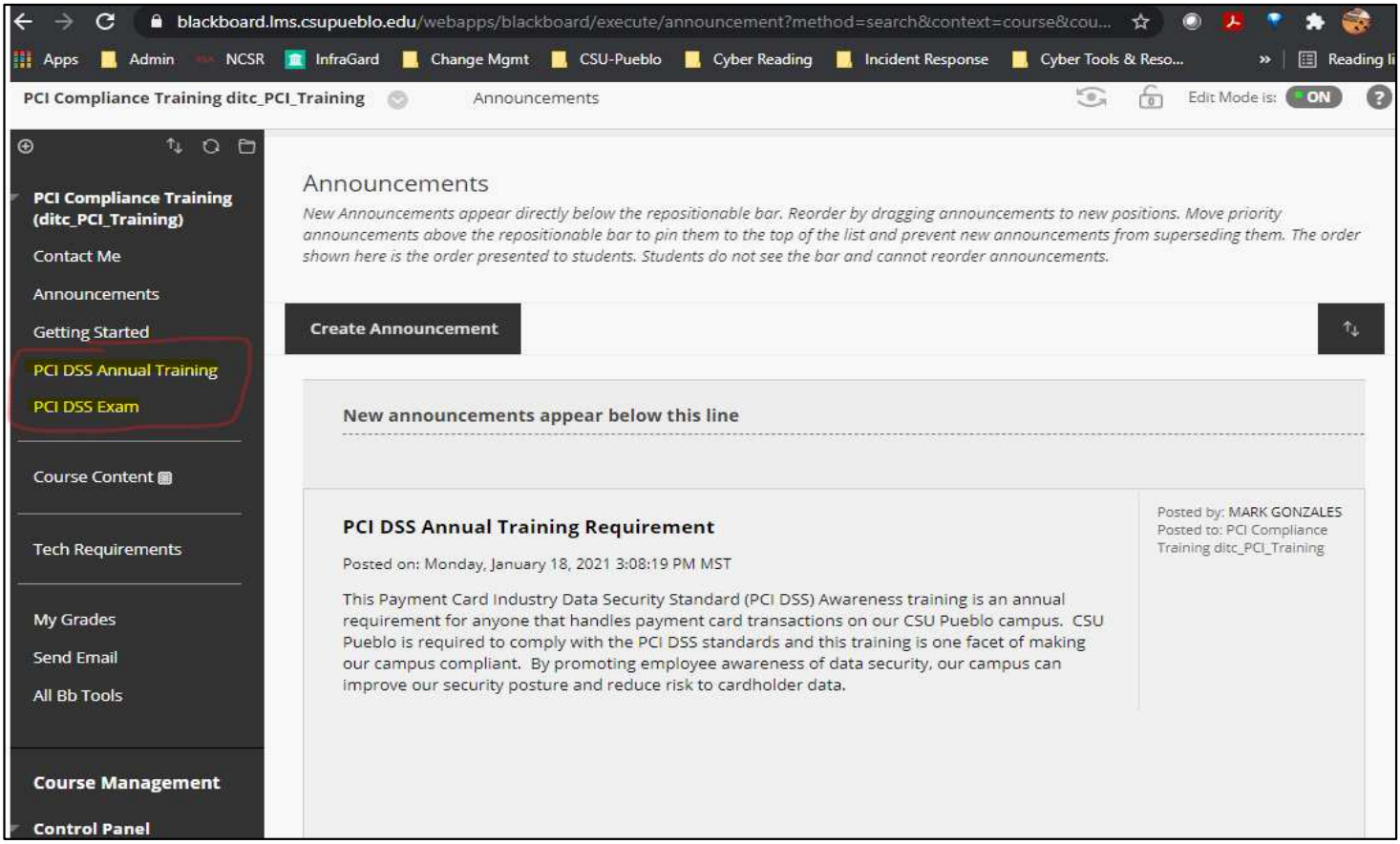
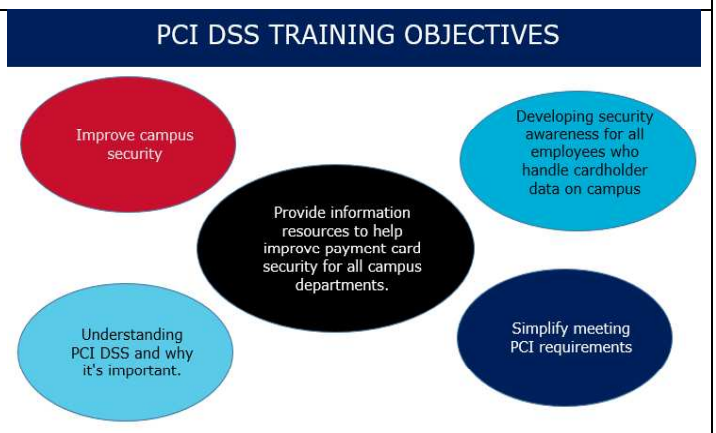


Image 2: PowerPoint training (Title Slide)

Image 3: PowerPoint training (Slide 1), Objectives



COLORADO STATE UNIVERSITY
PUEBLO

APPENDIX D

Information Security Working Group

Security is a culture. Cyber Protecting our university starts with this group.
We need your help.

MEETING INFORMATION

Date: March 25, 2021 (Reoccurring the last Thursday of the month)
Time: 3:00 to 3:50 PM

AGENDA

ISWG Security Questions/Concerns?

1) (Sarah) Is email from other legitimate schools allowed through our Mimecast email filter or is it blocked by default?

Answer: Emails from legitimate Internet *domain names are allowed through automatically. Out Mimecast email management system automatically blocks known bad Internet domain names. We can also manually enter in bad Internet domain names or even a bad actors email address so that we can prevent others on campus from getting phishing or email scams.

***GDPR and *CCPA in a nutshell = Data Privacy**

2) EverFi free GDPR training

Reminder: I'll be adding your names to the EverFi GDPR training with a due date of December 31, 2021. This is not a requirement so please let me know if you want me to take you off of the list.

3) Reminder: CSU Fort Collins has already done the heavy lifting for GDPR! https://gdpr.colostate.edu/

(Action Item: Mark) Copy the Privacy Areas and Controllers table from the https://gdpr.colostate.edu/ website and use it as a template for CSU Pueblo. Add in any other Services/Systems we offer.

(Action Item: Mark) Once the Privacy Areas and Controllers table is filled in then a meeting of those people needs to take place to ask them to describe the bulleted items.

i) Identifying Data Stewards
ii) Point of contact for each department
iii) Establish data retention period
iv) Periodic review of their data
v) Least privileges

Campus Situational Awareness

4) You might be hearing about DUO Multi Factor Authentication (MFA) on campus, what is it?

a) https://duo.com/product/multi-factor-authentication-mfa

5) IT Disaster Recovery VTTX 2021 After Action Report and Improvement Plan overview.

6) CSU System Cyber Consultation Kick-off meeting was March 22, 2021

Identifying where are we at now with our security posture on campus using the CIS Controls. The CIS Controls provide prioritized cybersecurity best practices. https://www.cisecurity.org/controls/

7) A window into how many security events our campus sees.

- Phishing attempts Jan thru today = 26
- Vendor related breaches = 1 (Mimecast)

How to determine if your email address and passwords have been leaked in a data breach:

(1) https://haveibeenpwned.com/

(2) https://monitor.firefox.com/

8) *PCI DSS (PCI) Compliance: Annual Audit and Training start now March 2021.

The PCI Audit is an annual internal audit that is required for all campus departments that handle credit card transactions or data. Outlook calendar invitations for the audit portion of our compliance have already gone out.

Part of our being compliant includes PCI training. This year, training has been setup in Blackboard. Anyone on campus that handles credit card transactions or data is required to take the training i.e. fac/staff/students. Please let me know if you have anyone that needs to take the training.

Communication Methods

9) Reminder: please send me your cell phone number in order to receive IT Emergency Messaging using the RAVE SMS services (Emergency Situations only).

10) Campus InfoSec Monthly Newsletter March https://www.csupueblo.edu/information-technology/security/newsletter.html

Cybersecurity Awareness

- Biggest data breaches February 2021
  - https://www.youtube.com/watch?v=gVV85InR6EM
- Cybersecurity in Education (Higher Education)
  - https://www.youtube.com/watch?v= x2F5FVG6R4

DEFINITIONS

GDPR	Genera Data Protection Regulation
CCPA	California Consumer Protection Act
PCI DSS	Payment Card Industry Data Security Standard
Internet Domain Name	An Internet domain name is a unique name of an organization or person on the Internet. For example, the Internet domain name for CSU Pueblo is https://www.csupueblo.edu/ and for Fort Collins it is https://www.colostate.edu/.

PURPOSE OF ISWG

- Consists of CSU **Pueblo faculty and staff**. Each team member is designated as their department point of contact for a Cybersecurity incident.
- **Provide a security vision for our campus.**
- **Raise Information Security awareness** for your departments and the campus as a whole.
- **Recommend Information Security (InfoSec) initiatives** to campus IT Governance committee.
- Act in a leadership role in **identifying improvements, strategies, projects, and policy** related to Information Security.
- **Provide InfoSec guidance for campus compliance** management related policies (e.g. FERPA, GDPR, HIPPA)
- **Assist with identifying campus critical systems** and prioritizing the order in which these critical systems will be brought back online.
- Assist with **drafting public information messaging.**
- Identify and **discuss legal issues** related to Information Security.
- **Protect our campus' ability to perform normal operations.**

Protect our data.
Protect our technology.
Protect our students, faculty, and staff.

CSU PUEBLO

COLORADO STATE UNIVERSITY
PUEBLO

APPENDIX E

CSU Pueblo IT **Information Security Team** Meeting

Cybersecurity teams are at the frontline

CSU PUEBLO

AGENDA

MEETING INFORMATION

Date: March 17, 2021 (3rd Wed of every month)
Time: 10:00 to 10:50 AM

TEAM MEMBERS

Blue italic text are notes taken during the meeting
Red italic text are action items

AGENDA

1. **Introduce new members/guests**
2. **Team Discussion: Team Questions and Concerns**
   - ☐ *(Frank, 2021feb17) with the increase demand for laptops, what is the policy for stolen laptops?*
     - (Mark) I've submitted a project through IT Governance to start using BitLocker and to use Active Directory to automatically store the keys.
     - [Action Item: Mark] Update CSU Pueblo written policy and include a pointer to CSU System website/FC policy.
     - Fac/Staff vs. Student employment laptop checkout is different.
     - IT Project BitLocker – easy setup for new machines, harder for machines existing machines.
   - ☐ Should these monthly meetings be an opportunity to train (EOC, Incident Response, COOP, DR) or should they be what they are now, a place to discuss security issues and concerns and campus updates?
     - Best of both – pre-read on campus IT Security updates and also a training opportunity. Have the full training at separate meetings. **This group is the Think Tank to identify trainings for IT, Leadership, Faculty, Staff, Students.**
3. **Global/Local Security Affecting Our Campus**
   - ☐ *Mimecast Data Breach Notification (Solarwinds Orion) – see below
   - ☐ Microsoft Exchange Zero-Day Webpage (aka Critical Patches) https://www.cisecurity.org/ms-exchange-zero-day/
4. **Campus Stats**
   - ☐ Phishing 2021
     - January = 16

     - February = 4
     - March (to date) = 6
   - ☐ Disaster Recovery AAR-IP waiting to hear back from IT Mgmt team before sending out.
     - [Action Item: Mark Close the loop with Lisa Gertig on the DR Audit
   - ☐ PCI Annual Department Audits starting March 23, 2021
   - ☐ CSU Pueblo IT Risk Assessment Consultation starting March 22, 2021 (CSU System auditors)
   - ☐ Windows 7 to Windows 10 Updates:
     - FacStaff = 306 Completed, 397 Errors
     - Student Labs = Starting March 31st (749 machines)
   - ☐ Windows 2003, 2008 servers: No update
   - ☐ GDPR Project: Not started
     - [Action Item: Mark] Identify Data Stewards from each campus department to assign take the EverFi GDPR training.
   - ☐ Incident Response Plan Exercise: Not started
   - ☐ Training:
     - Cybersecurity Awareness Packages for our Campus - InfoSec, Ninjio, KnowBe4, SANS
     - How to use an Emergency Operation Center

Important Security Update

e are reaching out to update you about the recent Mimecast security incident, which we determined was conducted by the me sophisticated threat actor responsible for the SolarWinds supply chain attack. We have recently completed our forensic vestigation into the incident with leading forensics and cyber incident response experts at Mandiant, a division of FireEye. We ll be making our incident report available via the Mimecast blog and the notification feed in the Administration Console by 12 n EDT on March 16, 2021.

ur recently completed forensic investigation with Mandiant showed us that the threat actor accessed certain data fields within r system related to your organization. **We have no evidence that the threat actor accessed email or archive content held y Mimecast on behalf of our customers.** Provided below are an overview of the data accessed and recommendations based n our risk-based analysis.

hat types of data were affected?
Email addresses and/or **display names** and/or **search terms** for no more than 10 of your Saved Searches, searches used in saved eDiscovery cases and exports, or searches initiated by users via our end user applications.

hat does this mean to you?
No action is required for your account.
As already mentioned, we have no evidence that the threat actor accessed email or archive content held by Mimecast on behalf of our customers, including any email content related to the search terms identified above.
For more information, see Saved Archive Searches.

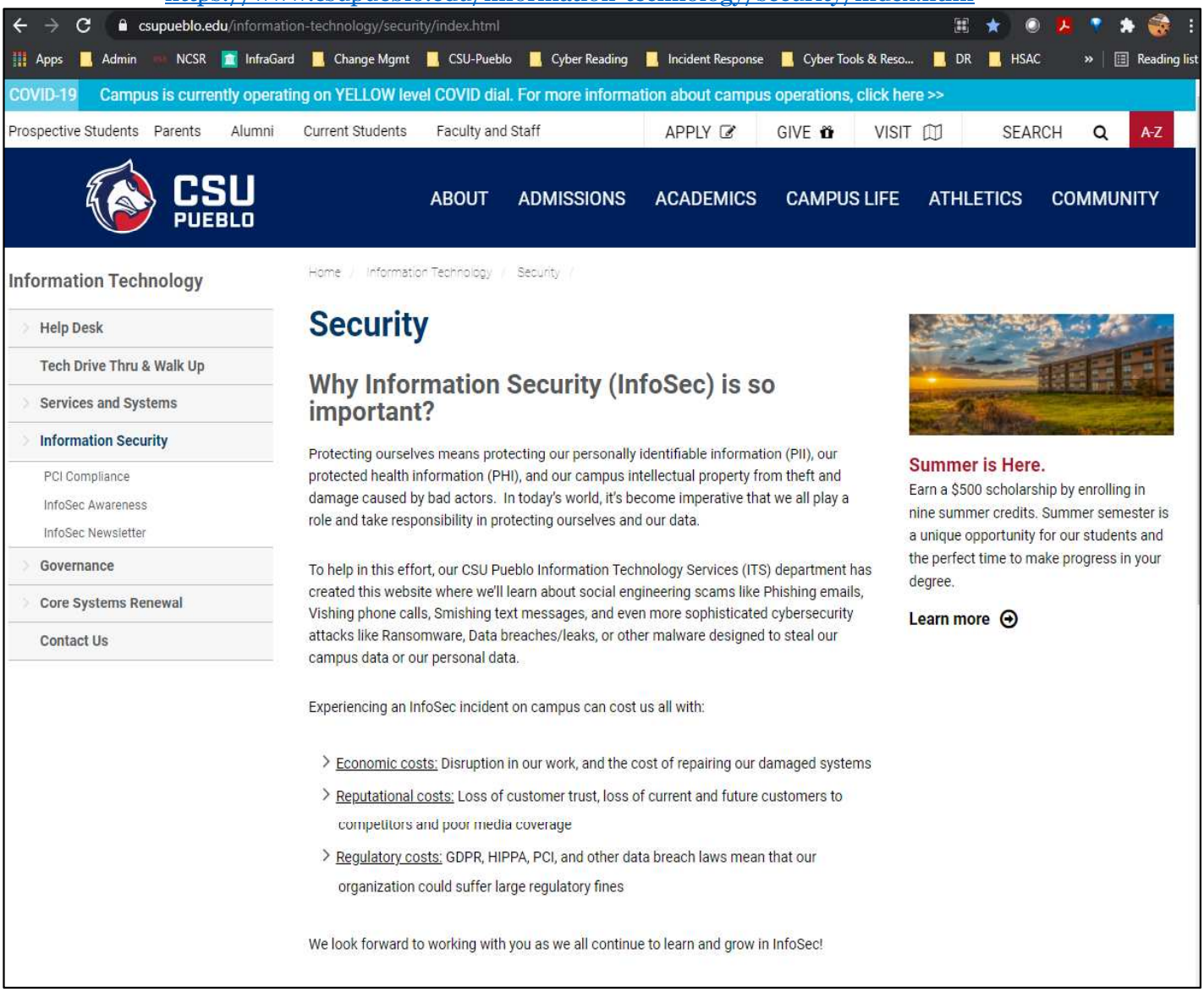
me stamp: Tuesday 16th March, 7.30AM EST, 11.30AM GMT

I Understand

COLORADO STATE UNIVERSITY
PUEBLO

APPENDIX F

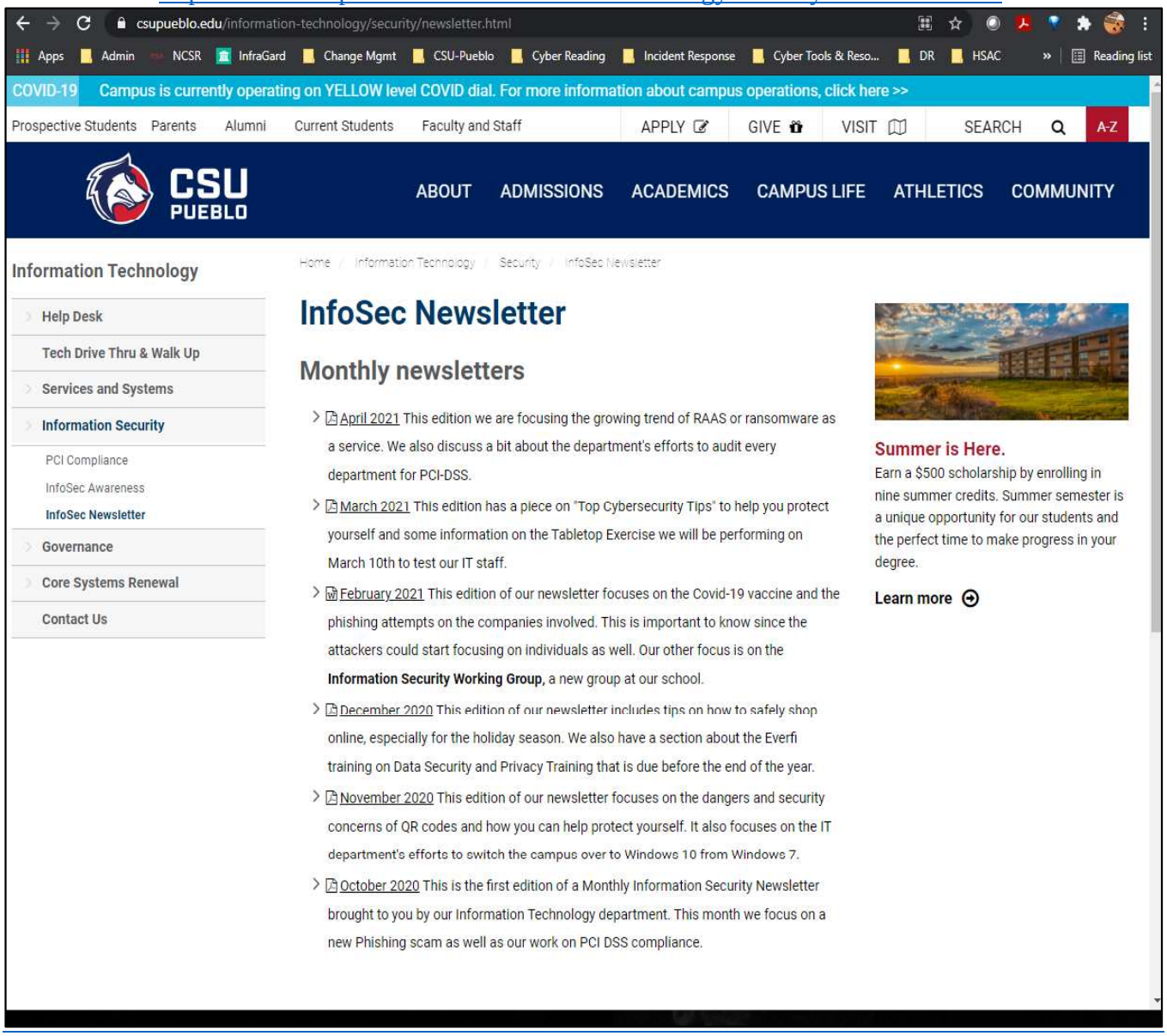
https://www.csupueblo.edu/information-technology/security/index.html



COLORADO STATE UNIVERSITY
PUEBLO

APPENDIX G

https://www.csupueblo.edu/information-technology/security/newsletter.html



MALIK AND SEEME HASAN SCHOOL OF BUSINESS

2200 BONFORTE BLVD.
PUEBLO, COLORADO 81001-4901
(719) 549-2142 Fax: (719) 549-2909

Colorado State University Security Resources, Security Awareness Programs

Information Technology Services – Computing Resources Agreement

Information Technology Services (ITS) at Colorado State University-Pueblo provides a broad spectrum of support for the planning, development, deployment, and integration of state-of-the-art facilities, infrastructure, and services to support the information technology needs of the academic, research, and administrative functions of the University. ITS provides oversight, management, coordination, integration, and staffing of Information Support Services, Instructional Technology Center, Network and Systems Services, Technology Support Services, and Telephone and Network Cabling Services.

To gain access to the university's computing resources, complete a *"Computer Resource Application"* **(http://www.csupueblo.edu/its/forms/)** and submit it to Information Technology Services in Administration Building Room 111. Computing resources such as the university's network, e-mail, Administrative Information System (AIS), and other university software will be established for you once this official form is received, Human Resources has received all required employment paperwork and, when applicable, a contract completed.

Each person granted access to university computing resources is responsible for adhering to ALL university technology policies. Pertinent policy information is available on the web at http://**www.colostate-pueblo.edu/its/**, and includes the following policies:

- **Electronic Communications Policy** — Guidelines established for the use of all electronic communications
- **Computer Account Policy** — Computer account & eligibility guidelines
- **Password Policy** — Guidelines established for the use of passwords
- **Electronic Mail Policy** — Use of electronic mail
- **Security Guidelines and Procedures** — Computer and network security guidelines and procedures
- **Computer Crime Policy** — Information about what constitutes computer criminal activity and penalties
- **Server Policy** — Governs the implementation of servers on the University network
- **Wireless Deployment Management Policy** — Provides information about the structure of the campus wireless technology
- **Web Page Guidelines** — Guidelines for developing web sites and pages
- **ResNet Policy** — Governs the use of Internet Services to on-campus residents.
- **Toll Free Number Policy** — Use of Toll Free telephone numbers on campus

If you need assistance using the university's computing resources, contact the Information Technology Services Help Desk at 549-2002. Hours of operation for the Help Desk are Monday through Friday, 7:30 am to 5:30 pm.

I agree to adhere to all University Technology Policies as indicated above and understand that failure to do so may result in the loss of my privileges to utilize the University's computing resources. I further understand that failure to adhere to the policies may result in corrective or disciplinary action up to and including termination.

Employee Signature _____ Date _____

Form: 4/2019

2021 HSB 119 and HSB 117 Lab and Applications Resources

Operating Systems

- **Dedicated Domain Controller (Running Win 2008)**
- **VM for Windows Server 2008-R2 and Server 2012**
- **VM Player**
- **Virtual Machine for Linux**
- **Virtual Machine for Win Server 2012**
- **VirtualBox**

General Applications

- **MS Office and Libre office application**
- **ABTutor**

Specialized Applications and Security Software

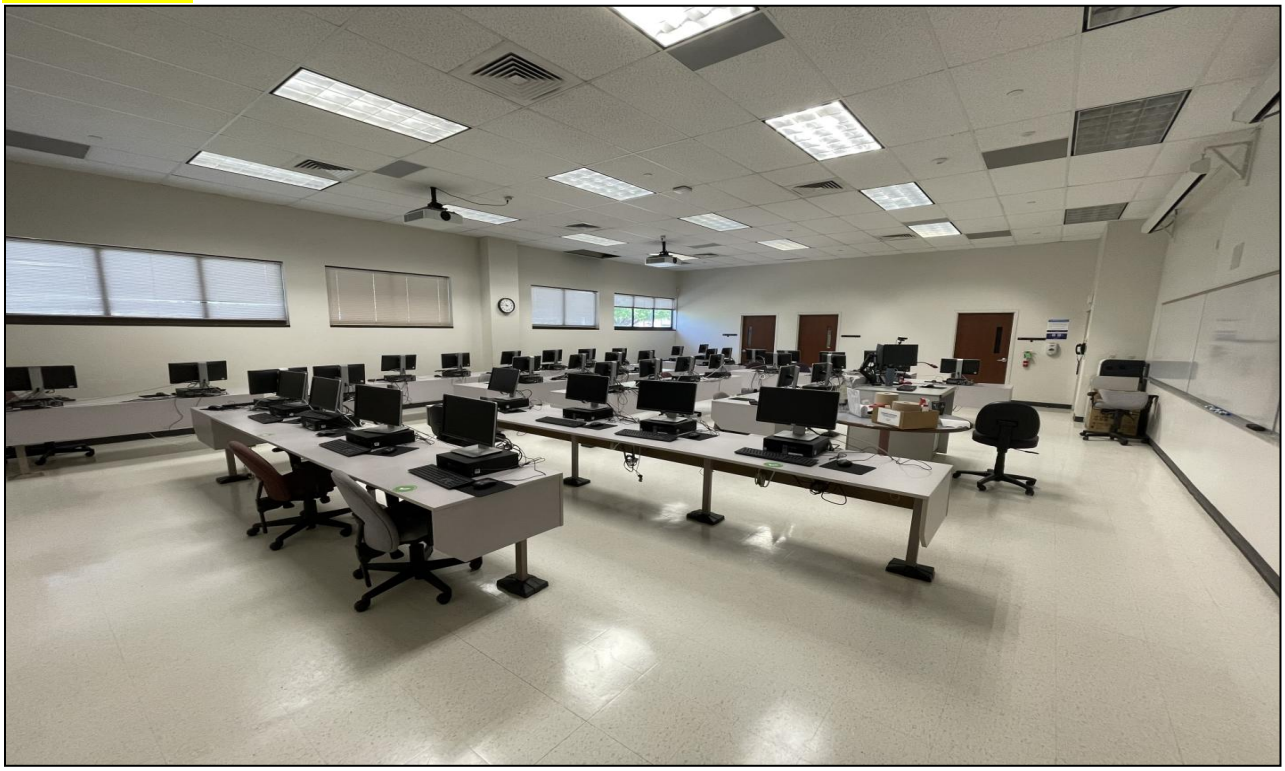
- **MS Project Professional**
- **MS Visio**
- **MySQL**
- **Heidi- SQL**
- **John the Ripper**
- **Kleopatra**
- **Helix**
- **Wireshark**
- **Nmap**
- **Sam Spade**
- **SuperScan**

HSB-117-General Computer Lab Resources

- **MS Office**
- **MS Project Professional**
- **MS Visio**
- **MySQL**
- **Heidi SQL**

Colorado State University-Pueblo
HSB LABS, May, 2021

HSB 117 Lab



HSB 119 Lab

Colorado State University-Pueblo

Cyber Security Weblinks + Intelligence Agency Publications and Research

All CSU-P Faculty, Staff and students have access to many subscription-based on-line Cyber Defense, Cyber Security, Information Security, System Security academic and practitioner journals, book and related publications. **https://www.csupueblo.edu/library/index.html**

Cyber-Security, Cyber Defense website, links
https://www2.fireeye.com
http://info.surfwatchlabs.com.
http://www.cybersecurityinformation.com/

Intelligence Agencies: *Research and Publications*

http://www.dhs.gov/topic/cybersecurity (CIS 460, click on Cyber Security Overview, for CIS 461, click Cyber Incident Response)

https://www.ivytech.edu/cyber-security/index.html (for Cyber Information Assurance (IA)

https://twitter.com/cyber_security (Links to various recent Cyber security breaches)

https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

Wireshark Tutorial
http://searchsecurity.techtarget.com/tip/Wireshark-tutorial-How-to-sniff-network-traffic

National Security Agency (NSA)
https://www.nsa.gov/ia/
https://www.nsa.gov/research/index.shtml **(NSA Research)**
https://www.nsa.gov/research/publications/index.shtml **(NSA Publications)**
https://www.nsa.gov/careers/index.shtml **(NSA Jobs and Careers)**
https://www.nsa.gov/ia/index.shtml **(Information Assurance)**
https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_Top10IAMitigationStrategies_Web.pdf **(Top 10 I.A. Mitigation Strategies)**
https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_SegregatingNetworksAndFunctions_Web.pdf **(NSA: Segregating Networks and Functions)**

Federal Bureau of Investigation (FBI)
https://www.fbi.gov/
https://www.fbi.gov/stats-services/publications **(FBI Report and Publications)**
https://www.fbi.gov/scams-safety **(Scams and Security)**
http://www.ic3.gov/default.aspx **(Reporting Internet Crimes)**

International Information System Security Certification Consortium (ISC)2
https://www.isaca.org/Pages/default.aspx

Central Intelligence Agency (CIA)
https://www.cia.gov/index.html
https://www.cia.gov/library/publications **(CIA Publications)**

Credit Card Fraud Stats
HTTP://WWW.STATISTICBRAIN.COM/CREDIT-CARD-FRAUD-STATISTICS/

Cyber Risk Mgmt / Disaster Recovery / Cyber Law

Cyber Risk Mgmt
Cyber Risk Network
http://www.cyberrisknetwork.com/

Information Systems Security Association
https://www.issa.org/

National Cyberwatch
http://www.nationalcyberwatch.org/

Contingency Planning/ Disaster Recovery/ Business Continuity
NIST Contingency Planning Guide for I.T. System (NIST 800-34)
http://ithandbook.ffiec.gov/media/22151/ex_nist_sp_800_34.pdf