The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.


mOASIS
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Header @ 1
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 1019971
Procurement Type: Central Contract - Fixed Amt
Vendor ID: VC0000027598
Legal Name: CAMPUSGUARD LLC
Alias/DBA:
Total Bid: $0.00
Response Date: 02/25/2025
Response Time: 10:28
Responded By User ID: jhaack
First Name: Jennifer
Last Name: Haack
Email: jhaack@campusguard.com
Phone: 6122076336
SO Doc Code: CRFQ
SO Dept: 0231
SO Doc ID: OOT2500000016
Published Date: 2/19/25
Close Date: 2/25/25
Close Time: 13:30
Status: Closed
Solicitation Description: Addendum No 1 Cybersecurity Privacy Training (OT25000)
Total of Header Attachments: 1
Total of All Attachments: 1

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder:	1619671
Solicitation Description:	Addendum No 1 Cybersecurity/ Privacy Training (OT25069)
Proc Type:	Central Contract - Fixed Amt

Solicitation Closes	Solicitation Response	Version
2025-02-25 13:30	SR 0231 ESR02252500000005202	1

VENDOR

VC0000027508
CAMPUSGUARD LLC

Solicitation Number: CRFQ 0231 OOT2500000016

Total Bid: 0 **Response Date:** 2025-02-25 **Response Time:** 10:28:50

Comments:

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor
Signature X **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Privacy and Cybersecurity Training Solution	1.00000	YR	0.000000	0.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments: Please refer to the attached proposal for complete pricing

Extended Description:

Specification 3.1.1. Vendor must provide a Lump Sum Cost for Year One Contract Services.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Privacy and Cybersecurity Training Solution-Optional YR2	1.00000	YR	0.000000	0.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments: Please refer to the attached proposal for complete pricing

Extended Description:

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Two Contract Services.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Privacy and Cybersecurity Training Solution-Optional YR3	1.00000	YR	0.000000	0.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments: Please refer to the attached proposal for complete pricing

Extended Description:

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Three Contract Services.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Privacy and Cybersecurity Training Solution-Optional YR4	1.00000	YR	0.000000	0.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments: Please refer to the attached proposal for complete pricing

Extended Description:

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Four Contract Services.

CampusGuard®

121 South 13th Street, Suite 102
Lincoln, Nebraska 68508

info@campusguard.com
www.campusguard.com

February 25, 2025

Toby Welch
State of West Virginia
2019 Washington St E
Charleston, WV 25305

Dear Toby:

CampusGuard is pleased to present this proposal to you and the West Virginia Office of Technology (WVOT). The services and pricing proposed in this document incorporate objectives as you have provided in the Request for Quote and based on CampusGuard's direct experience partnering with over 450 community-based institutions to achieve and maintain secure data.

CampusGuard is responding to the full Scope of Work as prescribed in your RFQ.

We look forward to partnering with you and WVOT and would appreciate an opportunity to meet with you and the committee members to discuss our response. If you have questions or require additional clarification of any element of this response, please contact me at 419.873.7016 or by email at agrant@campusguard.com. We look forward to your evaluation of our response and to the opportunity to discuss any aspect of our services.

Sincerely,

Andrew Grant, Director, National Business Development
CampusGuard
419.873.7016
agrant@campusguard.com

CAMPUSGUARD®

Response to Request for Proposal

CRFQ OOT2500000016
Cybersecurity/Privacy Training

Prepared for:

Toby Welch
State of West Virginia
304.558.8802
toby.l.welch@wv.gov

Prepared by:

Andrew Grant,
Director of National Business Development
CampusGuard
419.873.7016
agrant@campusguard.com

Table of Contents

Introduction

At CampusGuard, we deliver a unified approach to complex cybersecurity and compliance requirements to campus- and community-based organizations, including higher education, healthcare, and state and local government, among others. Our customer success is directly related to the experience and education of our certified professionals, our customer-centric approach, and our commitment to excellence.

Online Training Solution

The human factor is consistently identified as the weakest link in data security. It is critical for employees to receive effective security awareness training, so they have the knowledge and skills to help protect sensitive information from compromise and prevent potential cybersecurity incidents.

CampusGuard's online training solution allows WVOT to develop an effective and holistic security awareness and compliance training program, managed by our team of information security and compliance consultants. CampusGuard's expert team will help you create a customized training strategy to engage your employees and motivate them to implement information security best practices directly into their daily roles and responsibilities.

CampusGuard's courses are designed specifically for campus- and community-based organizations to provide all employees (and third parties) with the knowledge to protect and reduce the risk to sensitive information loss and theft. Our team closely monitors changes to industry requirements, trends, and emerging threats and all CampusGuard courses are updated ***annually*** with any changes in risks/technology, regulatory requirements, statistics, recent attacks, and lessons learned. This eliminates the need for internal resources and replaces inconsistent and outdated training. All course content is developed and reviewed by CampusGuard professional staff (certified security experts with credentials including QSA, CISSP, CISA, etc.). Courses are developed to address real pain points, challenges, and common gaps found within our compliance assessments to ensure training is relevant to employees and motivates them to prioritize security and change risky behaviors.

The CampusGuard Approach

CampusGuard is not just a training content provider. CampusGuard team will partner directly with your team to build a successful, customized awareness training program for WVOT and deliver measurable results. As many organizations do not have the time and/or resources to create and/or keep training up to date, let alone maintain a truly effective program, CampusGuard's team can ensure your users are receiving consistent and up-to-date training ongoing.

During the initial implementation process, we will work with you to review the available courses within the CampusGuard library and select the modules that are most applicable and/or required for the various departments and roles within WVOT. Our training consultants can help determine compliance training requirements (i.e., PCI DSS, GLBA, FERPA, HIPAA, etc.) and identify user groups that could benefit from specific training modules.

CampusGuard can help structure a schedule for rolling out the selected modules and topics based on user groups and roles, as well as appropriate training windows based on WVOT's calendar. Through micro-learning, WVOT can select specific topics to be shared with users monthly or quarterly as desired, and allow for more frequent training to ensure security awareness is kept top of mind for employees.

The CampusGuard team provides guidance on how to collect user information and what information may be helpful to track within training reports (i.e., department information, locations, supervisors, etc.). CampusGuard also provides templates to help structure enrollment notifications informing users of their training requirements and enforcement, reminder notifications, completion/certification emails, etc. We can also build in applicable policy acknowledgements to ensure users understand their individual responsibilities.

Following course implementation, the CampusGuard team will help measure overall user progress, as well as the effectiveness of the training by reviewing user participation, quiz scores, etc., and the level of engagement within your training program year over year. Through recurring quarterly touchpoint calls, we help monitor usage and ensure new employees are enrolled in the necessary training upon hire.

For any annual/ongoing training requirements, the CampusGuard team will contact the WVOT team to ensure the updated training content has been made available and is ready to deploy to your users well in advance of the required training window. CampusGuard will also provide guidance on supplemental training activities that can be shared outside of the standard training cycle.

Mandatory Requirements

Requirement	CampusGuard Response
The Privacy and Cybersecurity Training Solution must be an adaptive curriculum for Cybersecurity (Information Security) and Privacy training. The State of West Virginia must be able to customize the training topics.	✓
The Privacy and Cybersecurity Training Solution must provide integration with the State's current Active Directory environment.	✓
The Privacy and Cybersecurity Training Solution must have editable modules for the following topics, at a minimum: ▪ Understanding Security Threats ▪ Security Responsibilities ▪ Physical Threats ▪ Emergency Preparation ▪ Security Work Areas and Resources ▪ Access Controls ▪ Safe Computing and Electronic Threats ▪ Social Engineering Threats ▪ Password Guidelines ▪ Safe Remote and Mobile Computing ▪ Acceptable Use ▪ Phishing Identification and Preparation ▪ Responsible Social Networking ▪ Protecting and Handling Data ▪ Records Management and Data Classification ▪ Privacy Awareness and Privacy Principles (PII) ▪ Complying with PCI-DSS ▪ Complying with HIPAA ▪ Understanding PII ▪ Social Engineering ▪ Identity Theft ▪ Incident Reporting ▪ HIPAA Training, including: – What is HIPAA – Personal Health Identifying Information – Covered Entities – HIPAA Privacy Rule – HIPAA Security Rule – HIPAA Enforcement Rule – HIPAA Breach Notification Rule – The Importance of Confidentiality – The Minimum Necessary Standard – Business Associate Agreements – Patient Rights	✓ Please refer to the Courses section for a complete list of available modules. Each of your required topics are covered in one or more module.

The Privacy and Cybersecurity Training Solution must have the option to include Role Based Training.	✓
The Privacy and Cybersecurity Training Solution must support 25,000 active employees and on-site contractors.	✓
The Privacy and Cybersecurity Training Solution must be hosted in an LMS that is compatible with a SCORM 2.0 or higher.	✓
LMS must allow for additional 3rd party SCORM compliant courses to be uploaded	✓
LMS must be able to integrate with Microsoft Lightweight Directory Access Protocol (LDAP).	✓
The Privacy and Cybersecurity Training Solution must be branded with the West Virginia State Seal and Office of Technology Logos.	✓
The Privacy and Cybersecurity Training Solution must contain appropriate images to the training content and contain West Virginia-specific graphics.	✓
The Privacy and Cybersecurity Training Solution must contain a customer-customizable “Resources” section.	✓
The Privacy and Cybersecurity Training Solution must generate optional Certificates of Completion.	✓
The Privacy and Cybersecurity Training Solution must provide options for course rollout assistance, specifically: ▪ Launching an entire course ▪ Launching sections of a course ▪ Noting students as “passed” or “failed” ▪ Pass or failed percentage or score must be customizable	✓
The Privacy and Cybersecurity Training Solution must allow knowledge checks and graded assessments.	✓
The Privacy and Cybersecurity Training Solution must have a targeted length of at least 30 minutes, and no more than 45 minutes, of education content.	✓*
The Privacy and Cybersecurity Training Solution must provide a phishing simulator along with training if an end user fails the phishing simulation.	✓
The Privacy and Cybersecurity Training Solution must have predesigned and editable phishing templates for users conducting the simulation. ▪ Customization must be included for the email message itself along with attachments and web address the end user will click on. ▪ Predesigned templates must mimic current real-world phishing attacks.	✓
The Privacy and Cybersecurity Training Solution must support multi-factor authentication for log-in.	✓
The phishing simulator must integrate with Microsoft Lightweight Directory Access Protocol (LDAP).	✓
Provide reports, visualizations, and graphs showing user interactions. ▪ Reports must be able to be exported to popular file formats for distribution such as .pdf, .csv. ,xlsx, etc.	✓

▪ Reports must be able to generate reports for specific end-users or specific state.	
The phishing simulator must also include a reporting option for the end users to report phishing emails and track the reporting statistics for testing campaigns. ▪ The reporting option must be able to be utilized for all phishing emails reported to the Office of Technology. ▪ Be sure to describe and list all tools or processes that can be used to analyze malicious email with the reporting tool.	✓
The phishing simulator must have the ability to test for user input (i.e., the user clicks on a link and provides requested information to "scammers")	✓
The phishing simulator must support attachments.	✓
The phishing simulator must be able to provide, at a minimum, statistics on: users that clicked links and/or visited sites, provided credentials, opened or forwarded the email, time stamps for interactions, phishing training and test results.	✓
The phishing simulator must support phishing campaigns up to 5,000 users/email addresses.	✓
The phishing simulator must have end-user education options in the form of an educational landing page, reply email, or training module.	✓

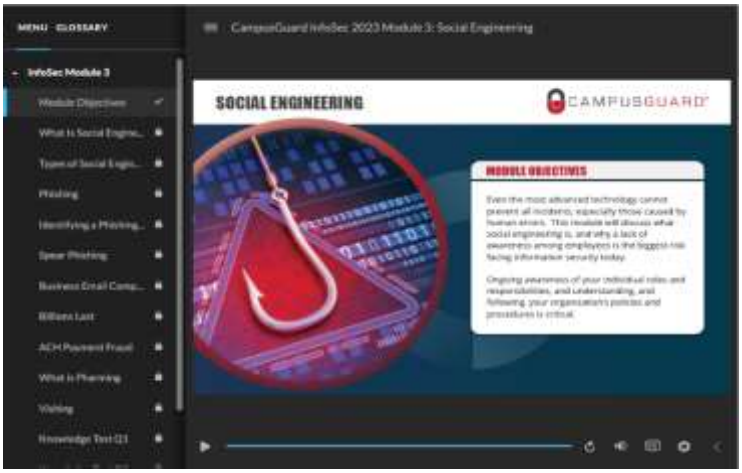
* CampusGuard's modules consist of micro learning modules (6-12 minutes in length). These micro modules allow you to provide simplified, more frequent training for staff versus lengthy, annual requirements. The flexible modules can also be structured and grouped accordingly to create a longer training course.

Course Structure

Format/Navigation

All CampusGuard courses have a visible table of contents that helps users understand where they are within a specific course. This table of contents also helps users track progress within each module. Each course also contains a glossary of key terms used within the modules. The navigation bar at the bottom of the screen allows users to view the training in full screen, start/stop the training, increase/decrease speed of the audio, move forward or back within the training, and review the closed captioning notes. This easy-to-use navigation allows users to pause a course and return to it later without losing their place.

We have designed the training content in a structured way that prevents users from fast-forwarding through the materials or allowing the course to play on another screen while they focus on other tasks. Preventing fast forwarding ensures users are engaged with the content, promotes increased comprehension and retention of the required information, and ensures users are not inadvertently missing crucial details.



All information on the module slides is concise, in large font, and easy to review/understand.

All course modules are interactive and require the user to engage on the screen with click throughs, games, and videos.

Assessments/Knowledge Tests

Each module also has a configurable. interactive knowledge test at the end to reinforce user understanding of the course materials and best practices and promote knowledge retention. The selected number of questions are pulled from a randomized test bank to ensure a varied assessment experience across learners. By default, most tests are configured with a passing threshold of 80% for assessments, however we understand WVOT may have specific requirements for determining completion of training modules and can provide flexibility to meet those preferences.

By default, learners must complete/pass the assessment in order to achieve course completion. This ensures learners have reviewed all content and can also demonstrate their understanding of key concepts. Courses can also be configured so that if a user does not achieve a passing grade upon the initial attempt, they can review the course content again before re-testing. This ensures learners have a solid comprehension of the course materials. Assessments are updated annually during the scheduled course updates to ensure learners are challenged and have an up-to-date understanding of risks and best practices. Customers can also optionally provide and create tailored assessments if needed to target specific roles or departments and align testing efforts with WVOT-specific policies and procedures.

Watch Video

Customization

CampusGuard understands that WVOT has unique requirements and specific roles within your workforce. Content can be branded and customized to align the solution with your look and feel and include information and links for association with WVOT's policies and procedures. This helps ensure all training aligns with current processes and presents a cohesive message to end users, allowing them to directly relate the training content back to their specific job roles and responsibilities.

With optional customization, the courses can also be configured to allow for a pre-course test-out option in which the user would be presented with a series of questions that must be answered accurately before moving into an abbreviated version of the course highlighting any WVOT-specific requirements that might need acknowledged.

During the implementation process, your CampusGuard team will provide documentation for your team to designate any requested module changes, links to organizational information, policy references, etc.

Accessibility

All CampusGuard training courses are designed with accessibility in mind and incorporate a user-friendly interface and customizable features including:

- Audio/narration for all slide content
- Closed captioning notes
- Keyboard progression functionality
- Clear navigation
- Page titles
- Use of color/contrast
- Text spacing/sizing
- Labels/instructions for all pictures

All courses are compliant with the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA and we can provide a Voluntary Product Accessibility Template (VPAT) upon request. The VPAT serves as a comprehensive assessment of our training courses' conformance with accessibility standards. Module transcripts can be provided in text format upon request.

Courses

The CampusGuard library consists of a diverse range of compliance-focused and information-security focused courses for adult learners. A consistent training approach is recognized across the various course topics to ensure a cohesive training program for WVOT.

Many of the courses also feature specific role-based modules which can be used to ensure users are receiving relevant training based on their daily roles and responsibilities.

The current Security Awareness and Compliance libraries include:

Information Security Awareness

CampusGuard's Information Security Awareness course consists of 18 micro learning modules (6-12 minutes in length). These micro modules allow you to provide simplified, more frequent training for staff versus lengthy, annual requirements. The flexible modules can also be structured and grouped accordingly to align with specific staff roles on campus.

- **Information Security (8 minutes):** This module will discuss what information security is, and why it is important to everyone. Training is designed to provide all employees who have access to WVOT's computer systems and networks, with the awareness and motivation to protect, and reduce, the risk associated with managing sensitive information.
- **Data Classification and Protection (6 minutes):** This module will discuss the classification of sensitive data types and various security and compliance requirements that WVOT is responsible for adhering to.
- **Social Engineering (12 minutes):** Statistics continue to indicate that a lack of awareness among employees is the biggest risk facing information security today. This module will review common social engineering attacks so users can more easily identify and protect WVOT against potential attacks. Phishing is a major focus of the training with an included sample email with warning indicators highlighted.
- **Email Security (7 minutes):** This module discusses email best practices along with prevention strategies for identifying and avoiding potential risks including spam messages, malicious attachments, and email hoaxes.
- **Password Management (6 minutes):** Strong passwords help to prevent unauthorized access to systems and information. This module covers password best practices, including password strength and management.
- **Remote Work Environments (9 minutes):** This module primarily focuses on remote work environments and understanding the risks and best practices for keeping data and devices secure when operating outside of the corporate environment.
- **Incident Management (7 minutes):** Incident management describes the activities to identify, analyze, and remediate a potential incident or compromise. This module reviews the difference phases of incident management and response, as well as lessons learned from recent breaches.

- **Internal Controls (6 minutes):** Internal controls include the policies and procedures WVOT uses to safeguard assets, ensure reliability and integrity of information, ensure compliance, promote efficient and effective operations, and accomplish operational goals and objectives. This module will review why just having policies in place for acceptable usage, least privilege, etc. is not sufficient alone, and why it is important that all users adhere to them.
- **Security Components (8 minutes):** Technical solutions to address security continue to evolve, and new products and versions are being released daily. This module discusses some of the common components used to secure devices and networks, including firewalls, intrusion detection systems, vulnerability scanning, anti-virus software, encryption, and multi-factor authentication.
- **Physical Security (7 minutes):** If physical access to sensitive information and/or systems is not restricted, unauthorized individuals could easily get their hands on this sensitive data. Best practices for physically securing your environment and basic steps for information storage and disposal are covered in this module.
- **Cyber Crime (16 minutes):** This module reviews some of the most common risks and threats to information systems, like malware, viruses, advanced persistent threats, bots, ransomware, crypto-jacking and more. Strategies for both proactively protecting systems and devices are discussed, as well as how to identify and report potential compromises.
- **Internet Usage (8 minutes):** This module reviews the importance of using common sense and following information security best practices when accessing the Internet. Topics reviewed include web browsing, cookies, cloud services, file-sharing and the Internet of Things.
- **Security at Home (8 minutes):** it is important for employees to understand the importance of protecting their home network, and ensuring the right tools are in place before accessing organizational resources. This module also reviews best practices for connecting to networks, installing applications, social networking, and more.
- **Data Breaches and Compromises (8 minutes):** With data breaches continuing to increase, it is critical organizations understand where the desirable data lives, what the risks are, and limit the risks as much as possible. This module will review weaknesses identified in recent breaches, as well as the average costs of a data breach.
- **Third-Party Risks (6 minutes):** While outsourcing services are chosen for a number of reasons, including increased efficiency, decreased cost, or a lack of internal resources, it doesn't come without risk. This module reviews why it is critical to properly evaluate third-party vendors, understand responsibilities, and implement a program to monitor their compliance on an ongoing basis.
- **Travel Security (8 minutes):** Traveling can pose a significant risk to information stored on or accessible through laptops, tablets, and smartphones. This module reviews steps to protect employee devices and sensitive information before and during potential business travel.
- **Artificial Intelligence (8 minutes):** AI, or Artificial Intelligence, if used appropriately, can be a valuable business tool. Applications can be used to automate tasks, analyze data, generate reports, and even detect fraud. However, before any AI applications are implemented for organizational use, it is important to understand any associated security risks. This module

will provide users with an understanding of Artificial Intelligence and usage and discuss requirement to ensure AI is used in a way that aligns with industry best practices, privacy and consumer protection regulations, and organizational policies and procedures.

- **Help Desk Security (12 minutes):** Help desks have become a common point of entry for hackers attempting to gain access to organizational systems and/or data. This module provides users with an understanding of social engineering risks targeted at help desk staff, necessary processes for verification of callers, incident reporting and response, how to monitor help desk calls, and best practices for new system updates and/or applications.

Watch Video

Phishing Awareness

This course is designed to help your staff understand the common goals and strategies found within phishing campaigns and how to proactively identify red flags and phishing indicators within email messages. Training users to detect and react to phishing attacks will help protect WVOT from potential security incidents. Training can be used as part of your general awareness training or as supplemental training modules to be assigned to users that respond to test phishing messages. Modules include:

- Phishing 101
- Rules for Spotting Phishing
- Phishing Practice

Watch Video

PCI DSS Compliance

- **PCI for Merchants (45 minutes):** Comprehensive overview of the Payment Card Industry Data Security Standard (PCI DSS) requirements, including best practices how to protect cardholder data, securely process payment card transactions on campus, and meet the ongoing compliance requirements from the DSS. Modules include:
  - Introduction to PCI DSS
  - Payment Card Security
  - Identifying Risks
  - Compliance with PCI DSS
- **PCI for Students/Cashiers (15 minutes):** Training to meet the requirements of the Payment Card Industry Data Security Standard (PCI DSS) requirements and educate front-line staff on how to securely handle cardholder data and process payment card transactions.
- **PCI for Executives (20 minutes):** High-level overview of the Payment Card Industry Data Security Standard (PCI DSS) requirements, including best practices on how to securely handle cardholder data, how to protect cardholder data, and how to securely process payment card transactions.

- **PCI for E-commerce (20 minutes):** Training focused for those merchants that are not involved in the day-to-day processing of cards, but rather have an online store or ecommerce site their department manages or supports. Module reviews best practices for securing online storefronts and monitoring third-party relationships.
- **PCI for IT (60 minutes):** This course provides a closer look at the Payment Card Industry Data Security Standard, and the requirements WVOT needs to meet prior to attesting annual compliance. This training is geared towards IT staff and management, who, while not typically participating in the payment process, are responsible for implementing and maintaining the required technical infrastructure campus-wide. Modules include:
  - PCI DSS Compliance
  - Securing the Cardholder Data Environment (CDE)
  - Objectives and Requirements

Watch Video

GLBA

- **Introduction to GLBA (13 minutes):** This training module provides an overview of GLBA and its application within higher education, discusses increasing information security risks, and strategies for protecting sensitive data, penalties for non-compliance and the possible consequences of a data breach.
- **Privacy Rule and Safeguards Rule (12 minutes):** This module covers both the GLBA Privacy Rule and the Safeguards Rule, the required administrative, technical, and physical controls that must be implemented, necessary third-party oversight, and steps to achieve compliance.

Watch Video

FERPA

- **Introduction to FERPA (17 minutes):** This training course provides an overview of the Family Educational Rights and Privacy Act (FERPA) and the laws governing acceptable use and release of student education records. The course reviews individual staff and faculty responsibilities, provides guidance on how to protect students' right to privacy, and explains the potential consequences of non-compliance.
- **Common Scenarios (8 minutes):** Module discusses several different scenarios in which a faculty or staff member may be requested to share student information. Users must review the situations carefully and select the appropriate answer. Training provides a comprehensive explanation to help guide users in their FERPA awareness.

Watch Video

FACTA Red Flags

- **FACTA Red Flags Overview (20 minutes):** This course is designed to help your staff prevent fraud and identity theft. The module provides an overview of the Fair and Accurate Credit Transactions Act (FACTA) and the associated Red Flags Rule, discuss strategies for identifying and detecting potential fraud, raises employee awareness of suspicious information and activities, explains how to handle notices or alerts of identity theft, and details procedures for responding to red flag incidents.

  Watch Video

HIPAA Compliance

- **Introduction to HIPAA (5 minutes):** This module provides an introduction to HIPAA, why it was created, and changes to the law in recent years. The training will provide an introduction to HIPAA, why it was created, and changes to the requirements in recent years.
- **Protected Health Information (5 minutes):** What information does HIPAA protect? This module discusses Protected Health Information (PHI), the identifiers that are required to be protected under HIPAA, and what information may be considered exempt.
- **Who is Required to Comply with HIPAA (6 minutes):** This module reviews the three categories of covered entities, as well as requirements for third-party business associates. Training also discusses the impact of HIPAA within higher education.
- **HIPAA Privacy Rule (7 minutes):** This module reviews the different components of HIPAA. Training discusses the interrelated Privacy Rule, including key components and patient rights. At a high level, the Privacy Rule covers Personal Health Information in all forms, while the Security Rule covers only electronic PHI or ePHI.
- **HIPAA Security Rule (12 minutes):** The Security Rule outlines three types of safeguards required for compliance: administrative, physical, and technical. Training provides end users with guidance around password security, physical security, information disposal, and the protection of health records.
- **Risks to PHI (12 minutes):** This module covers common risks and threats to HIPAA environments, and best practices for protecting PHI data. Training reviews common HIPAA violations and walks through several practice scenarios to test users' ability to identify and prevent potential violations.
- **Data Breaches and Reporting (7 minutes):** In this module, we will discuss best practices that should be implemented to prevent potential data compromise. Examples of data breaches and response efforts will be reviewed in detail.
- **HIPAA Enforcement (6 minutes):** In this final module, we will common HIPAA violations and OCR enforcement for noncompliance. The training concludes with the recommended steps for achieving and maintaining HIPAA compliance.

  Watch Video

Resource Library

Each information security and compliance course set also has a related Resource Library of supplemental content (handouts, posters, articles, etc.) that can be shared with users as part of ongoing awareness campaigns, in monthly newsletters, or posted in offices to help reinforce key messages and best practices. New resources are added throughout the year by the CampusGuard team to allow your teams to engage users ongoing, provide up to date, current information, and build a culture of security awareness across the organization.

Technical Information

SCORM

Course files can be delivered as Shareable Content Objective Reference Model (SCORM) SCORM 1.2 or SCORM 2004 files for Customer to upload and direct use in your internal Learning Management System (LMS). Our SCORM packages are fully compliant with SCORM specifications and compatible with a wide range of LMS platforms. All SCORM content is published as Scalable HTML5 content and is compatible with modern browsers (Chrome, Firefox, Safari, Edge, etc.) supported by the developer, as well as accessible on mobile device browsers, both iSO and Android.

Through the SCORM course file, we have options to report back to the LMS platform a user as either “Complete/Passed” or “Incomplete/Fail”. Interaction data and slide views are reported directly to the LMS. Completion criteria can be based on percentage of slides viewed by the learner and/or when the learner completes a knowledge test with a pre-defined passing percentage/score. Each course module contains a knowledge test (pulled from a test bank) to measure end user understanding. Quiz scores and specified interaction data can also be reported and shared with the LMS platform. CampusGuard will provide necessary title information, class description, and training hours for configuration within the LMS platform.

SCORM files can be provided for each individual module within a course, or WVOT can elect to combine multiple modules to be delivered as a single course to assigned users.

CampusGuard courses are tested using SCORM Cloud. Courses are also uploaded into the CampusGuard training platform prior to release and undergo a thorough QA cycle to ensure seamless integration with your Learning Management System (LMS). As industry updates are made, and new versions of common browsers are released, CampusGuard tests course functionality. A sample SCORM file can be provided upon request so WVOT can test for usability/compatibility within the internal LMS.

CampusGuard-Hosted Platform

Online training courses provided via our fully hosted, robust learning management system. The learning platform is web-based and compatible with all modern browsers, including Firefox, Edge, Chrome, Safari, and Opera. The platform is also compatible with all browsers used by the latest mobile devices (i.e., iOS and Android).

Platform Branding

Customer can select to have CampusGuard brand their platform with custom images, logo, and color scheme.

User Access

Licensed users access the platform using their secure login ID and a one-time password of which they will change to something personal upon initial login. CampusGuard's training platform also supports single sign on through SAML 2.0 identity provider.

Users can self-register for courses, but the platform will enable organizational administrators to approve or deny the requested user before access is granted.

User Roles

Users can be assigned either a user role or an administrator role. Administrative access allows a customer admin to add and maintain users, assign courses, and view on-demand progress reports for users by individual course or across WVOT.

Reporting

An intuitive administrative dashboard allows your team to easily measure the ongoing effectiveness of your training and monitor staff participation. Training administrators can review progress reports detailing user enrollments and completion dates/progress. Progress reports can be exported on-demand from the platform or configured to be emailed out to applicable contacts via email at a defined timeframe (i.e., progress report sent every Monday). Administrators can customize report fields to drill down based on user departments, locations, supervisors, job title, course assignments, etc.

Notifications

Each course can have customized notifications configured for initial enrollment, course completion, and course reminders (weekly, bi-weekly, etc.) until the user completes the required training. These email notifications can be customized to communicate any specific training requirements, due dates, enforcement, etc.

Certificates of Completion

Users receive a customized certificate of completion following each course. Certificates can be downloaded by the individual users or by administrators on-demand. Users will also have access to a printable or downloadable transcript that outlines all completed and in process, assigned courses.


[Organization]

Certification

This certification is awarded to

[First name] [Last name]

For successfully completing the course

[Course]

[Latest issue date]

Issued Date: Date is displayed as MM/DD/YYYY

[Expiration date]

Expiration Date: Date is displayed as MM/DD/YYYY

CAMPUSGUARD

Support

The CampusGuard Training product is supported by a team of CampusGuard customer relationship managers which manage the overall relationship with each organization, along with a dedicated Operations Support team to help address any user questions, set up customized progress report options, and coordinate with your teams on new training launches. All courses go through a thorough quality assurance process internally prior to annual release.

CampusGuard's Operations Support team is available Monday-Friday (8:00-5:00 CT) via email and/or phone to assist with any user support or troubleshooting and all inquiries can expect a response within 12 hours, but typically within 1 hour. Platform has greater than 95% uptime and can ensure the training materials are available to users on a 24/7 basis.

CampusGuard offers two levels of our hosted platform:

CG-Hosted Standard

Online Training Packages are hosted on CampusGuard's Training Platform and the customer performs all user additions, deletions, and changes outside of the annual user bulk load. WVOT administrators will have the ability to add, edit, and inactivate users as needed or assign users to courses/modules. Spreadsheets of users for import from each specific business/employer can also be provided directly to the CampusGuard Operations Support team for enrollment.

CG-Hosted Premier

Online training packages are hosted on CampusGuard's Training Platform and CampusGuard support personnel perform all user additions, deletions, and changes, plus a variety of additional support activities outlined in the Online Training Packages table below to help WVOT build a comprehensive and cohesive training program and measure success ongoing.

Features	SCORM	Standard Hosted	Premier Hosted
Annual course content updates by credentialed security experts	X	X	X
Pre-built templates for course notifications and acknowledgements	X	X	X
Pre-built learner assessments/knowledge tests to confirm user understanding of best practices	X	X	X
Access to Compliance and InfoSec Resource Libraries	X	X	X
Bi-monthly Threat Intel newsletter	X	X	X
Quarterly touchpoint call with Training Administrator to review feedback/questions	X	X	X
Administrator dashboard and training		X	X
Customizable administrator roles		X	X
On-demand and scheduled course progress reports to primary administrators		X	X
Evaluation of compliance training requirements		X	X
Automated and customizable user notifications (enrollment, reminders, completion, etc.)		X	X
Customized policy/procedure acknowledgement		X	X
Annual user updates/course rollouts as new course content is available		X	X
User support (troubleshooting/access)		X	X
Customer administration of ongoing user maintenance (adding users, inactivating users, moving departments, assigning courses)		X	X
Structure annual training calendar/schedule for the organization			X
Identify user groups for course assignments/role-based training – customizable training program by group			X
Customized course progress report for defined departments, managers, etc.			X
Learning Analysis – measure user participation and level of engagement (monitor usage across departments/locations)			X
Customized user analytics/training reports for annual board security updates			X
User surveys to gather user feedback			X
Customized training campaign materials (posters, handouts, messaging for staff) – Branded content			X
Optional Services			
Customized training course content to align with organizational policies and procedures	X	X	X
Braining Training Platform		X	X
Single Sign On Integration (Azure, SAML, etc.)		X	X
API Integration with Active Directory (user provisioning)		X	X
Integration with CampusGuard Central Platform		X	X
Quarterly Password Audits	X	X	X
Quarterly Phishing Tests	X	X	X
Facilitated Cybersecurity Incident Response/Tabletop Exercises	X	X	X
Compliance and Information Security Policy/Procedure Template Library	X	X	X
Compliance and Security Assessments	X	X	X

Platform Security

The security and privacy of your user information is not only important to us; that is the sole reason CampusGuard was founded, to help organizations protect sensitive information.

CampusGuard's learning platform has completed a compliant SOC 2 Type 2 examination for Security, Availability, and Confidentiality. CampusGuard can also provide a completed Higher Education Community Vendor Assessment Toolkit (HECVAT) so you can rest assured all information, data, and cybersecurity policies are in place to protect your data.

We have deployed a role-based access control system, and users are granted access based on their assigned roles and responsibilities. Permissions will be granted and revoked as per defined roles, preventing unauthorized access and minimizing the risk of system misuse. The platform also provides auditable logs/trails to track and record all activities related to the system.

Integrations

Single sign-on (SSO) is a highly secure user authentication process. SSO lets users access multiple applications with a single account and sign out instantly with one click. CampusGuard's hosted training platform supports single sign on through SAML 2.0 identity provider.

User provisioning lets you synchronize user accounts between the CampusGuard Platform and your IdP through the SCIM v2 API. This can reduce time spent on user maintenance and ensure the centralization of your users' access privileges. Common uses include pushing new users to the platform, activating or deactivating users, and updating user profiles automatically.

Customer Expectations

WVOT should provide a campus liaison who will serve as the primary contact for the project (managing billing, implementation, roll-out, ongoing maintenance, etc.)

Implementation

Upon contract, CampusGuard provides a smooth and effective onboarding process and partners with you to ensure a seamless implementation of the purchased training courses. Each CampusGuard customer is assigned a dedicated Customer Relationship Manager (CRM) as the point person throughout the duration of the contract to ensure all of your required needs are met. Once engaged with your team, the CRM will schedule a kick-off meeting with you to review the implementation plan and answer any questions. During this call, the CRM will verify course subscriptions, access, contact information for organizational resources, billing, etc. Following this call, the CRM will provide documentation outlining each of the courses and content for your team to review and outline any requested changes and/or customizations, as well as select the course modules your team would like to deploy.

Following this step, the CampusGuard training team will work to build the custom course(s) and develop a draft schedule for deployment. Once the draft course is ready for review, WVOT can view the completed course within the CampusGuard LMS and verify if there are any additional changes. Adjustments or changes in course titles, navigation menu, notes, etc. can be made during this review stage. Once the course is approved, the SCORM file(s) will be shared with WVOT for use in their internal LMS. CampusGuard will work with the team to ensure all reporting and completion updates are functioning as designed to ensure a seamless user experience.

Each CRM carries the PCIP credential from the PCI Council and is internally educated on other compliance standards. The CRM also works closely with our Operations Support team staff who will be assisting with course updates, uploading SCORM content, etc.

Following implementation, the CRM will also schedule planned, recurring meetings with your team to address any questions, review project milestones, progress reports, etc., and inform Customer of all updates related to the information security and compliance courses and platform enhancements as relevant to your project. Your CRM will also ensure you are receiving the necessary support and assistance for your learners through the contract term and can coordinate with our Operations Support team, as well as other CampusGuard teams as needed.

As an additional service, the CampusGuard Security Advisor team and/or the RedLens Information Security team are available to help answer technical or compliance-specific questions you may have, help build customized phishing campaigns, and/or partner with WVOT on more detailed social engineering/penetration testing to identify any potential gaps and weaknesses within your information security program.

References

Reference 1	
Customer Name	State of Hawaii Department of Business, Economic Development & Tourism
Contact	Jason Ushijima
Phone	(808) 265-4921
Email	Jason.s.ushijima@hawaii.gov
Reference 2	
Customer Name	State of Delaware Office of the Treasurer
Contact	Vivek Maharaj
Phone	(302) 672-6732
Email	Vivek.maharaj@delaware.gov
Reference 3	
Customer Name	Marshall University
Contact	Jon Cutler
Phone	(304) 696-3270
Email	Jon.cutler@marshall.edu

Cost Proposal

OLT Package	InfoSec Awareness Package	Compliance Package	Both Packages	Single Compliance Course
# of Licenses	**100**	**100**	**100**	**100**
SCORM – per license	$22.00	$22.00	$25.00	$16.00
CG HOSTED – per license	$30.00	$30.00	$33.00	$24.00
CG Premier Support – per license	$32.00	$32.00	$35.00	$26.00
SCORM – Total Annual Price	$2,200.00	$2,200.00	$2,500.00	$1,600.00
CG Hosted – Total Annual Price	$3,000.00	$3,000.00	$3,300.00	$2,400.00
CG Premier Support – Total Annual Price	$3,200.00	$3,200.00	$3,500.00	$2,600.00
# of Licenses	**200**	**200**	**200**	**200**
SCORM – per license	$18.04	$18.04	$20.50	$13.12
CG HOSTED – per license	$24.04	$24.04	$26.50	$19.12
CG Premier Support – per license	$26.04	$26.04	$28.50	$21.12
SCORM – Total Annual Price	$3,608.00	$3,608.00	$4,100.00	$2,624.00
CG Hosted – Total Annual Price	$4,808.00	$4,808.00	$5,300.00	$3,824.00
CG Premier Support – Total Annual Price	$5,208.00	$5,208.00	$5,700.00	$4,224.00
# of Licenses	**300**	**300**	**300**	**300**
SCORM – per license	$14.79	$14.79	$16.81	$10.76
CG HOSTED – per license	$19.79	$19.79	$21.81	$15.76
CG Premier Support – per license	$22.79	$22.79	$24.81	$18.76
SCORM – Total Annual Price	$4,437.84	$4,437.84	$5,043.00	$3,227.52
CG Hosted – Total Annual Price	$5,937.84	$5,937.84	$6,543.00	$4,727.52
CG Premier Support – Total Annual Price	$6,837.84	$6,837.84	$7,443.00	$5,627.52
# of Licenses	**400**	**400**	**400**	**400**
SCORM – per license	$12.13	$12.13	$13.78	$8.82
CG HOSTED – per license	$16.13	$16.13	$17.78	$12.82
CG Premier Support – per license	$20.13	$20.13	$21.78	$16.82
SCORM – Total Annual Price	$4,852.04	$4,852.04	$5,513.68	$3,528.76
CG Hosted – Total Annual Price	$6,452.04	$6,452.04	$7,113.68	$5,128.76
CG Premier Support – Total Annual Price	$8,052.04	$8,052.04	$8,713.68	$6,728.76
# of Licenses	**500**	**500**	**500**	**500**
SCORM – per license	$10.31	$10.31	$11.72	$7.50
CG HOSTED – per license	$14.31	$14.31	$15.72	$11.50
CG Premier Support – per license	$18.31	$18.31	$19.72	$15.50
SCORM – Total Annual Price	$5,155.29	$5,155.29	$5,858.29	$3,749.30
CG Hosted – Total Annual Price	$7,155.29	$7,155.29	$7,858.29	$5,749.30
CG Premier Support – Total Annual Price	$9,155.29	$9,155.29	$9,858.29	$7,749.30

OLT Package	InfoSec Awareness Package	Compliance Package	Both Packages	Single Compliance Course
# of Licenses	**750**	**750**	**750**	**750**
SCORM – per license	$9.49	$9.49	$10.78	$6.90
CG HOSTED – per license	$13.49	$13.49	$14.78	$10.90
CG Premier Support – per license	$17.49	$17.49	$18.78	$14.90
SCORM – Total Annual Price	$7,114.30	$7,114.30	$8,084.43	$5,174.04
CG Hosted – Total Annual Price	$10,114.30	$10,114.30	$11,084.43	$8,174.04
CG Premier Support – Total Annual Price	$13,114.30	$13,114.30	$14,084.43	$11,174.04
# of Licenses	**1,000**	**1,000**	**1,000**	**1,000**
SCORM – per license	$8.73	$8.73	$9.92	$6.35
CG HOSTED – per license	$12.73	$12.73	$13.92	$10.35
CG Premier Support – per license	$16.73	$16.73	$17.92	$14.35
SCORM – Total Annual Price	$8,726.88	$8,726.88	$9,916.90	$6,346.82
CG Hosted – Total Annual Price	$12,726.88	$12,726.88	$13,916.90	$10,346.82
CG Premier Support – Total Annual Price	$16,726.88	$16,726.88	$17,916.90	$14,346.82
# of Licenses	**1,250**	**1,250**	**1,250**	**1,250**
SCORM – per license	$8.29	$8.29	$9.42	$6.03
CG HOSTED – per license	$12.29	$12.29	$13.42	$10.03
CG Premier Support – per license	$16.29	$16.29	$17.42	$14.03
SCORM – Total Annual Price	$10,363.17	$10,363.17	$11,776.32	$7,536.85
CG Hosted – Total Annual Price	$15,363.17	$15,363.17	$16,776.32	$12,536.85
CG Premier Support – Total Annual Price	$20,363.17	$20,363.17	$21,776.32	$17,536.85
# of Licenses	**1,500**	**1,500**	**1,500**	**1,500**
SCORM – per license	$7.88	$7.88	$8.95	$5.73
CG HOSTED – per license	$11.88	$11.88	$12.95	$9.73
CG Premier Support – per license	$15.88	$15.88	$16.95	$13.73
SCORM – Total Annual Price	$11,814.01	$11,814.01	$13,425.01	$8,592.01
CG Hosted – Total Annual Price	$17,814.01	$17,814.01	$19,425.01	$14,592.01
CG Premier Support – Total Annual Price	$23,814.01	$23,814.01	$25,425.01	$20,592.01
# of Licenses	**1,750**	**1,750**	**1,750**	**1,750**
SCORM – per license	$7.56	$7.56	$8.59	$5.50
CG HOSTED – per license	$11.56	$11.56	$12.59	$9.50
CG Premier Support – per license	$15.56	$15.56	$16.59	$13.50
SCORM – Total Annual Price	$13,231.69	$13,231.69	$15,036.01	$9,623.05
CG Hosted – Total Annual Price	$20,231.69	$20,231.69	$22,036.01	$16,623.05
CG Premier Support – Total Annual Price	$27,231.69	$27,231.69	$29,036.01	$23,623.05

OLT Package	InfoSec Awareness Package	Compliance Package	Both Packages	Single Compliance Course
# of Licenses	**2,000**	**2,000**	**2,000**	**2,000**
SCORM – per license	$7.26	$7.26	$8.25	$5.28
CG HOSTED – per license	$11.26	$11.26	$12.25	$9.28
CG Premier Support – per license	$15.26	$15.26	$16.25	$13.28
SCORM – Total Annual Price	$14,517.05	$14,517.05	$16,496.65	$10,557.86
CG Hosted – Total Annual Price	$22,517.05	$22,517.05	$24,496.65	$18,557.86
CG Premier Support – Total Annual Price	$30,517.05	$30,517.05	$32,496.65	$26,557.86
# of Licenses	**3,000**	**3,000**	**3,000**	**3,000**
SCORM – per license	$6.68	$6.68	$7.59	$4.86
CG HOSTED – per license	$10.68	$10.68	$11.59	$8.86
CG Premier Support – per license	$14.68	$14.68	$15.59	$12.86
SCORM – Total Annual Price	$20,033.53	$20,033.53	$22,765.38	$14,569.84
CG Hosted – Total Annual Price	$32,033.53	$32,033.53	$34,765.38	$26,569.84
CG Premier Support – Total Annual Price	$44,033.53	$44,033.53	$46,765.38	$38,569.84
# of Licenses	**5,000**	**5,000**	**5,000**	**5,000**
SCORM – per license	$6.01	$6.01	$6.83	$4.37
CG HOSTED – per license	$10.01	$10.01	$10.83	$8.37
CG Premier Support – per license	$14.01	$14.01	$14.83	$12.37
SCORM – Total Annual Price	$30,050.30	$30,050.30	$34,148.07	$21,854.76
CG Hosted – Total Annual Price	$50,050.30	$50,050.30	$54,148.07	$41,854.76
CG Premier Support – Total Annual Price	$70,050.30	$70,050.30	$74,148.07	$61,854.76
# of Licenses	**7,000**	**7,000**	**7,000**	**7,000**
SCORM – per license	$4.81	$4.81	$5.46	$3.50
CG HOSTED – per license	$8.81	$8.81	$9.46	$7.50
CG Premier Support – per license	$12.81	$12.81	$13.46	$11.50
SCORM – Total Annual Price	$33,656.34	$33,656.34	$38,245.84	$24,477.34
CG Hosted – Total Annual Price	$61,656.34	$61,656.34	$66,245.84	$52,477.34
CG Premier Support – Total Annual Price	$89,656.34	$89,656.34	$94,245.84	$80,477.34
# of Licenses	**10,000**	**10,000**	**10,000**	**10,000**
SCORM – per license	$3.56	$3.56	$4.04	$2.59
CG HOSTED – per license	$7.56	$7.56	$8.04	$6.59
CG Premier Support – per license	$11.56	$11.56	$12.04	$10.59
SCORM – Total Annual Price	$35,579.56	$35,579.56	$40,431.31	$25,876.04
CG Hosted – Total Annual Price	$75,579.56	$75,579.56	$80,431.31	$65,876.04
CG Premier Support – Total Annual Price	$115,579.56	$115,579.56	$120,431.31	$105,876.04

Notes:

1. A customer buys either an InfoSec Awareness Package, a Compliance Package, both full packages, or single compliance course/bundle.
2. SCORM = OLT Packages are hosted on Customer LMS
3. CG Hosted = OLT Packages are hosted on CampusGuard LMS and customer performs all user additions, deletions and changes outside of the annual user bulk load
4. CG Premier Support = OLT Packages are hosted on CampusGuard LMS and CampusGuard personnel performs all user additions, deletions and changes + additional resources (outlined in OLT service levels table).
5. CampusGuard reserves the right to audit subscriptions usage at each customer-hosted (SCORM) environment every six months.
6. Custom content can be delivered to each customer. The first five hours of custom content is delivered at $1600.00. Hours following the five hours can be completed at $325 per hour.
7. For CampusGuard Hosted customers a onetime custom OLT branding can be completed at $1195.00.
8. For CampusGuard hosted OLT customers a onetime single sign-on service can be completed at $2,495.00.
9. For CampusGuard hosted OLT customers a onetime AD/LDAP integration can be completed at $2,495.00.
10. All Phishing campaigns are billed at a fixed price using an hourly rate of $275.00. An average phishing campaign is about 25 hours per the CampusGuard typical deliverables.
11. Based on the number of campaigns needed pricing is negotiable.

OLT Definitions

Module: Lesson within a course, with a quick knowledge test following each individual module. Modules can be assigned individually or as a grouping, so organizations can schedule annual, quarterly, or monthly awareness training for staff.

Course: Offered training course specific to a compliance or information security topic (i.e., GLBA, FERPA, HIPAA, etc.) – subscriptions are purchased for a course.

Bundle: Group of courses available for a specific compliance topic (i.e., PCI DSS Compliance bundle consists of the PCI for IT, PCI for Merchants, PCI for Execs, PCI for Cashiers, and PCI for eCommerce).

Package: A selection of courses that can be purchased together at a packaged/discounted price (i.e., CampusGuard offers the Infosec Package which includes all Infosec course modules and Phishing course modules, or the Compliance Package which includes access to all compliance courses and modules (FERPA, HIPAA, PCI, FACTA, GLBA)).