MAKES TEACHING
AND LEARNING EASIER

canvas

www. | instructure.com

Instructure Security, Engineering, and Operations

Canvas Security

Instructure, Inc.

26 November 2014

TABLE OF CONTENTS

1 CANVAS SECURITY INFRASTRUCTURE

The Canvas education technology platform and learning management system is hosted on the state-of-the-technology cloud infrastructure provided by Amazon Web Services (AWS). The AWS infrastructure is highly stable, fault-tolerant, and secure as attested by the following certifications:

- SOC 2 Type I report using the Service Organization Control framework put forth by the American Institute of Certified Public Accountants (AICPA)
- Certified ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements
- Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS)
- Federal Information Security Management Act (FISMA) Moderate Authorization and Accreditation received from the U.S. General Services Administration.

For additional information about AWS security certifications and standards compliance, please refer to http://aws.amazon.com/security and http://aws.amazon.com/compliance/.

1.1 AWS Network Security

The AWS cloud infrastructure provides extensive network and security monitoring systems to protect the Canvas production environment and its data. These systems protect against:

- **Distributed Denial Of Service (DDoS) Attacks**. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.
- **Man In the Middle (MITM) Attacks**. All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. Amazon Elastic Compute Cloud (EC2) Amazon Machine Images (AMIs) automatically generate new Secure Shell (SSH) host certificates on first boot and log them to the instance's console.
- **IP Spoofing**. Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
- **Port Scanning**. When port scanning is detected, it is stopped and blocked.

1.2 AWS Services

The AWS services used to host Canvas include Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Simple Storage System (S3), Elastic Block Store (EBS), Virtual Private Cloud

(VPC), Simple Email Service (SES), CloudFront, Identity and Access Management (IAM), DirectConnect, and CloudSearch. All Canvas application nodes are hosted on the Amazon EC2 and S3 infrastructure, making full use of the real-time redundancy and capacity capabilities. Virtualization is provided by Amazon EC2.

1.3 AWS Regions and Data Centers

Amazon EC2 is hosted in multiple locations world-wide. These locations comprise regions and Availability Zones. Each region is a separate geographic area and each region has multiple, isolated locations known as Availability Zones. Instructure uses five AWS regions: the US East (Northern Virginia) Region with 5 EC2 Availability Zones, the US West (Oregon) Region with 3 EC2 Availability Zones, the EU West (Ireland) Region with 3 EC2 Availability Zones, the Asia Pacific (Sydney) Region with 2 EC2 Availability Zones, and the Asia Pacific (Singapore) Region with 2 EC2 Availability Zones.

AWS data centers utilize state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards and access is authorized strictly on a least privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. Multiple geographic regions and Availability Zones provide resilience in the face of most failure modes including natural disasters or system failures.

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Generators provide back-up power for the data centers of the entire facility.

1.4 AWS Data Security

All data traffic in and out of Canvas is at least 128-bit TLS/SSL-encrypted over HTTPS connections. Data is stored redundantly in the Amazon S3 infrastructure across and multiple geographic regions and multiple data centers. Canvas data is replicated in near real-time on the Amazon S3 infrastructure and is also backed up on a daily basis to geographically separate locations. Daily backups of Canvas data include media, file system data, course structures, coursework, analytics, rubrics, learning outcomes, and metadata. Canvas data replication and backups ensure that, in the event of a necessary system restore, the potential data loss would be limited.

2 CANVAS SYSTEM SECURITY

Canvas has been designed to achieve a high level of security by providing an uncomplicated, usable approach to user authentication, system access, and role-based, hierarchical permissions. Canvas is designed to support institution's own internal security policies and to provide rigorous protection from internal or external intrusions. Canvas reinforces system security by presenting a simple security model to end-users because research shows that if users have to jump through too many security hoops, they will attempt to find ways to bypass security entirely.

2.1 Identity and Access Management

Canvas supports centralized identity management and delegated authentication via integrations with external identity providers (IdPs) including Lightweight Directory Access Protocol (LDAP), Active Directory, Central Authentication Service (CAS), Security Assertion Markup Language (SAML) 2.0, and Shibboleth. Canvas supports federated identity management and Single Sign-On (SSO) via integrations with SAML, Shibboleth, and CAS. Additionally, user ID and password credentials from any third-party system can be synchronized with Canvas-internal, local authentication via the Canvas open API.

Canvas-internal authentication can be used alone or concurrently with any of the supported external IdPs identified above. For example, when used concurrently with LDAP, Canvas first presents user credentials to the external IdP. If authentication fails, Canvas then looks up the credentials using its internal authentication service. If authentication fails again, Canvas will deny the user login.

Canvas clients are encouraged to use Canvas in concert with their preferred external idP in order to best control and establish end-user security protocols. For Canvas-internal authentication, passwords must be 6 or more characters. Passwords are never stored in plain text. Passwords are securely hashed via the SHA-512 cryptographic hash algorithm with a randomly generated "salt" value. The resulting signature and salt value are then stored. When users attempt to authenticate, their credentials are passed through the same process and the resulting signature is checked against the stored signature. This process is exclusively uni-directional and passwords cannot be derived from their stored signature.

2.2 Protocol and Session Security

Canvas uses HTTPS (HTTP over TLS/SSL) for all communication. All inbound and outbound traffic is encrypted using 128-bit TLS/SSL ensuring that all personally-identifiable information, credentials exchange, page requests, and session data are secure.

Sessions are maintained and can be invalidated in the Canvas infrastructure. An encrypted session cookie, signed with a hash message authentication code (HMAC), is used only identify

a current session. The HMAC and cookie contents are encrypted with Advanced Encryption Standard (AES)-256 in cipher feedback (CFB) mode. The contents of the cookie cannot hijacked during transmission across the network, cannot be viewed or tampered with by the user, and cannot be accessed through javascript. Session IDs are compared and validated against the server-stored values. An invalidated session will require a user to login again.

Sessions are reset on each successful login to prevent access to session IDs by subsequent logins. To prevent cross-site request forgery (CSRF) vulnerabilities, all user actions that modify data require a session secret key to post data. All requests that modify data are done with HTTPS POST or PUT requests, never GETs.

2.3 Preventing Cross-Site Scripting (XSS) Attacks

Canvas employs a variety of strategies to prevent cross-site scripting (XSS) attacks. For example, when Canvas creates a form for user input, a one-time use token is embedded in the HTML form so that Canvas can identify the form and verify that it did not originate another site in a possible attack attempt.

As another example, because user-supplied JavaScript present a critical security vulnerability, Canvas does not allow non-administrative users to embed JavaScript directly into any Canvas pages. If, for example, a student were able to add JavaScript to a page, the student could embed code that changes the student's grade when the instructor visits the page without the instructor detecting it. For this reason, only Canvas account administrators can add custom JavaScript.

Canvas sanitizes content to protect against intentional or unintentional vulnerabilities. When content is put into a Canvas form, such as content that a user enters with the Rich Content Editor, Canvas scrubs the content and removes any of malicious content. Content sanitization prevents session jacking, form hacks, and other unauthorized data access and/or modifications.

All user-inputted content is sanitized server-side—*not* in JavaScript which can be bypassed—before it is saved to the database. The sanitization is done by explicit whitelisting, not blacklisting. This prevents the addition of JavaScript to HTML data and prevent the addition of the unsafe HTML tags as well.

2.4 File Upload and Download Security

User-uploaded files are stored in the Amazon S3 infrastructure with unique names and folders. To prevent side-jacking from user uploaded files and preserve the integrity of the system, Canvas places uploaded files in the Files repository under a different subdomain to establish a separate security domain in order to take advantage of the browser's same-origin security measures. The browser will enforce security between the uploaded files and the user's session and prevent session jacking. If an uploaded file executes code using JavaScript, Java, Flash, or

other technologies, that code will not be able to access the user's session nor be able to make requests to Canvas on the user's behalf.

All file downloads require unique, short-lived authorization keys.

2.5 Data Security

Instructure has developed custom code to validate that all Canvas data models are protected against invalid assignment. For example, no user can change foreign keys arbitrarily and all lookups are scoped to the appropriate current user and context. All SQL is built using placeholders and a framework for escaping user input; strings are never directly interpolated or concatenated.

The Canvas API provides secure access to Canvas data and functionality while preventing direct access to Canvas databases. The Canvas API uses the industry-standard OAuth2 protocol which allows third-party applications to access data and perform actions on behalf of users without ever having possession of the user's password. Users that use the API can revoke access to specific applications at any time.

2.6 Database Connection Security

Application servers communicate with the database via a "bouncer," a database proxy that handles connection pooling. Connections between the application servers and the bouncer as well as between the bouncer and the databases are over a heavily firewalled virtual network. The protocol spoken is the PostgreSQL secure TCP/IP with TLS/SSL protocol.

2.7 Data Security through Redundancy and Versioning

To protect against malicious or accidental data destruction, Canvas stores data redundantly and employs soft-deletions. Administrators and instructors can recover previous versions of the gradebook, content pages, and assignment submissions.

Instructure maintains versions of all Canvas data and content by taking a series of periodic snapshots of databases. Snapshots of databases are taken daily and each daily snapshot is retained for a week. Weekly snapshots are taken and retained for a month. Monthly snapshots are taken and retained for a year.

2.7.1 Canvas Disaster Recovery

Most structured data—courses, user information, and assignments—is stored in a PostgreSQL database. This data is horizontally partitioned between instances based on account and demand. Each partition has a primary and a secondary or replica database, located in geographically separate sites. The data from each primary is replicated asynchronously in near-

real time to its corresponding secondary. Each primary is also backed up completely every 24 hours, and the backup is stored in a third geographically separate site.

Files for static assets from courses and assignments are stored on a scalable, protected, geographically redundant storage system of the Amazon S3 infrastructure. Multiple copies are stored by Instructure for backup.

3 CANVAS SECURITY AUDITS

3.1 Internal Security Audits

Instructure's security team conducts quarterly internal security audits of the Canvas code base and Instructure's production environment. Members of Instructure's security team have many years of experience with security audits by major corporations and government agencies. Audit policies and procedures are reviewed on a regular basis and updated as needed by the security team.

The Instructure security team conducts thorough, comprehensive, prescriptive, internal security audits at least once a quarter. In these quarterly audits, the security team:

- Uses different development teams to do both Black Box and White Box testing.
    - In Black Box testing, developers presume no prior knowledge of the code or the inner workings of the application and then attempt to discover and exploit security vulnerabilities by a variety of methods. Black Box testing requires developers to think like a hacker. "How would I break into this system? How would I steal this data?"
    - In White Box testing, developers use their prior knowledge of the code and the inner workings of the application to test methods that could be exploited externally too. Developer reads through the application source code, looking for vulnerabilities at a low level.
- Scans the application externally, using off-the-shelf tools.
- Documents potential vulnerabilities, recommends fixes, and implements the most advantageous fix. The fixes are then retested, by both the original discoverer(s) and other, new-to-the-problem team members.
- Pushes fixes made in external libraries to the upstream development activities to be immediately applied and included in official packages instead of waiting for the next scheduled Canvas update release.

Instructure encourages all clients to subscribe to the Canvas Security Advisory Forum at http://help.instructure.com/forums/20382721-security-notices where security notices from internal security reviews, scanning, and testing are published.

3.2 External Security Audits

In addition to our frequent internal security audits conducted throughout the year, Instructure conducts annual, open, third-party security reviews. The 2013 review was conducted by the security company, Secure Ideas, in November 2013 and the results are available at http://www.instructure.com/downloads/Instructure_Canvas_Security_Summary_2013.pdf.

The open, external security audit is one way that Instructure can demonstrate not only the state of Canvas security, but also our responsiveness to any vulnerabilities. For example, in that audit, Securus Global identified three high-risk vulnerabilities in Canvas itself and in the underlying libraries Canvas uses. Instructure fixed those vulnerabilities on the same day that Securus Global reported them and Instructure issued security bulletins to our customers. And because Canvas is a true multi-tenant application, Canvas clients never experience the adverse effects due to unapplied updates or patches due to version differences or added costs or wait times for service packs.

This same level of responsiveness is applied when Instructure receives external input on security outside of the formal audit process. For example, in January 2013, a Rails SQL security vulnerability was identified. Instructure patched this vulnerability within a couple of hours with no downtime. Instructure Engineering also provided the updates Canvas source code on Github at the same time. Additional details are available on the Instructure Security Advisory Forum at: http://help.instructure.com/entries/21563740-instructure-advisory-iac56413-rails-sql-injection-vulnerability.

In addition, because Canvas is open source, anyone may audit the Canvas code at anytime. Multiple institutions and other entities have conducted their own independent security audits of the code. If and when security defects or vulnerabilities are discovered, Instructure's engineers work closely with these parties to resolve any discovered flaws. For customers who are interested in conducting their own security audit of Canvas, Instructure will, upon request, set up an environment, where they can conduct automated and manual vulnerability scanning.

4 INSTRUCTURE INTERNAL SECURITY

Instructure uses commercially reasonable efforts to provide logical and physical security designed to maintain the integrity of the logical and physical security of its internal systems and customer data and content.

4.1 Instructure Certifications

Instructure is SOC 2 Type 1 certified, an audited report on management's description of a service organization's system and the suitability of the design of controls. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16).

4.2 System and Data Access Policy

Instructure uses a multiple approval system for granting access to employees. First, the manager of the employee requesting access must fill out a ticket requesting detailed level of access to the system and specifying which parts, functions, and features are to be accessible by the employee. Clear, valid, and necessary business justification must be provided for the user in question.

The completed access request ticket is then routed to the Director of Operations. If approved by the Director of Operations, the request ticket is routed to the Operations team for final approval. If all parties approve the employee's access, the Operations team grants access as requested in the ticket. Per the employee exit policy, user accounts are deleted upon termination of employment.

All on-boarded Instructure employees are required to read, understand, and sign Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Act (COPPA) compliance forms.

4.2.1 Cryptographic Keys

Instructure's Operations team controls generation and installation of keys for all employees with access to the servers. An automated configuration system (Puppet) installs employee public keys on a per-server basis based on need. This same configuration process automatically revokes keys globally when necessary. Employees are required to use full-disk encryption and password protection on their work machines to protect their private keys and other sensitive data. The private keys used for HTTPS are stored encrypted and decrypted by operations when deployed to the application servers.

Monitoring and alerts are in place to detect and warn of any changes to keys, users on the system, login and sudo attempts, and other events of concern.

4.2.2 Physical Security

Access to Instructure's offices is controlled using access cards. Instructure restricts access to internal servers by physical locks. Instructure uses commercially reasonable efforts to protect client data behind a secure firewall system, to conduct daily data backups, and to store weekly full-system backups in a separate, fire-resistant facility.

4.2.3 Secure Coding and Development Practices

Maintaining and enhancing security is a disciplined, continual, and ongoing process. Secure coding and security testing are, therefore, integral components of Instructure's engineering and development methodology. All code in the application must go through a developer peer review process before it is merged into the code base repository. The code review includes security auditing are based on the Open Web Application Security Project (OWASP) secure coding and code review documents and other community sources on best security practices.

All Canvas developers are trained to identify and analyze security issues when writing and reviewing code. Members of the core security team and the engineering team subscribe to security-focused lists, blogs, and other resources to maintain, expand, and share the collective body of knowledge. Instructure maintains an internal wiki to discuss and share best practices for the mitigation and prevention of security pitfalls and vulnerabilities. The security and engineering teams keep up-to-date on general security practices, on recent attack vectors, and on any security issues specifically related to the languages, web applications, frameworks, and environments that Instructure employs to develop, host, and maintain Canvas.

Peer reviews of all source code changes are mandatory. Multiple peer reviews are conducted for each change to the Canvas code base to detect and correct any bugs, security flaws, and any other code defects. Changes to Canvas code must be validated by peer review *before* the code is approved and committed to the code base repository.

4.2.4 Testing and Quality Assurance

Once new code has passed peer review, the code is incorporated into the code base and submitted to testing and quality assurance. The new code is deployed to a continuous integration server where it is immediately tested. Instructure's testing team runs:

- Unit tests (testing code with code)
- Integration tests (testing code with integrations with other code)
- Selenium tests (testing how code works in the browser) on all the different environments and across different databases.

After passing these tests, the code is incorporated in the main Canvas development code for formal quality assurance (QA). The QA team tests the new code on all supported platforms and browsers.

4.3 Instructure's Response to Security Alerts

Unlike traditional LMS licensed products with service packs which often do not address security problems for weeks or months and which must be applied by the users themselves, Canvas is a cloud service with a single version of the code base and production environment so that security updates are immediately and automatically applied for the entire client base as part of Instructure's hosting services.

Regular vulnerability scans of the Canvas application and infrastructure are conducted using third-party tools (for example, Burp Suite Pro), custom scripts, and open source tools. If any vulnerabilities are detected, Instructure's security and engineering teams work together to analyze, design, and develop the required patch. Security-related patches to the operating system, application software, and libraries are applied within one (1) week except in those cases which have been determined to be high severity. If a high-severity security vulnerability is detected, fixing the vulnerability is given the highest priority by Instructure's security and engineering teams. High-severity security patches will be applied within twenty-four (24) hours by best commercial efforts. In most cases, the vulnerability can be fixed using a hot patch without incurring any downtime to the Canvas production environment.

Instructure, in coordination with AWS, takes a proactive approach to enforcing SAS 70 Type II controls. Postmortems are convened after any significant operational issue, regardless of external impact, and Cause of Error (COE) documents are drafted so the root cause is captured and preventative actions are taken in the future. Implementation of the preventative measures is tracked during Instructure's weekly operations meetings.

5 DATA EXPOSURE RESPONSE POLICY AND PLAN

Data security and safeguarding users' privacy are paramount concerns of Instructure. Instructure has implemented a comprehensive set of security technologies, management and review policies, monitoring operations, and enforcement procedures to ensure that our system and data security meets or exceeds governmental statutes and regulations, industry standards, and institutional requirements.

5.1 Data Exposure Response Policy

Backing up these preventative measures, Instructure has established a set of prescriptive responses to be executed in the event of unauthorized data exposure. Data exposure occurs when restricted or confidential information is disclosed, exposed, or reasonably believed to have been disclosed or exposed to an unauthorized person, process, or system.

Instructure's data exposure policy has been designed to ensure:

- Earliest possible detection of a system or data security breach;
- Rapid securing of the system and data to prevent further unauthorized exposure;
- Responsive notification to users and other affected parties that confidential or personal information has been or may have been exposed or compromised by a breach in system security.

5.2 Data Exposure Response Plan

In the event of a breach of security and potential unauthorized data exposure, the information security officer will oversee and execute a plan of action that conforms to the guidelines described in the subsections below. The exact plan of action to be executed and the sequence of the actions taken will depend on the type and scope of the breach in security.

5.2.1 Determine the Scope of the Security Breach

In all cases, the information security officer and staff will quickly assess the status of the breach to determine whether the activity is ongoing. If the activity is ongoing, the security staff will take immediate requisite measures to stop the unauthorized activity in order to prevent any further data loss. Once the breach is isolated and stopped, the information security officer and staff will begin to ascertain the extent of the breach, the source and type of data involved, the amount of data, and the affected persons and system resources.

5.2.2 Assemble an Incident Response Team

The information security officer will assemble an incident response team. The composition and charge of the team will depend upon the type of breach and resulting data exposure. The team will conduct a preliminary assessment and risk assessment and help develop a tailored incident response plan. Once the incident is contained, this team will also evaluate changes in processes, systems and/or policies to prevent a repeat event.

5.2.3 Control Dissemination of Information

In order to ensure that only accurate, timely information that will not interfere with the ongoing investigation is released, only the information security officer will be authorized to provide information to any party outside of the incident response team.

5.2.4 Alert Administrative Team

The information security officer will alert the appropriate senior administrators including the Instructure executive team, client institution officials, system engineers, and other key players as warranted.

5.2.5 Identify Affected Persons

The information security officer will work with institution officials, Instructure's VP of Engineering, Instructure's Director of Operations, and the incident response team to determine the identities of affected individuals and determine the extent of the data exposure.

5.2.6 Notify Affected Persons

The information security officer will work with the VP of Engineering, Legal, Director of Operations, and the incident response team to draft and execute a notification plan. The purpose of the plan is to provide full, accurate, and timely notification that meets or exceeds all statutory requirements. In the case of high severity security issues, affected parties will be alerted immediately while indirectly affected parties will be alerted within twenty-four (24) hours. These legal requirements will vary on a state-by-state basis. Working with the appropriate parties, The information security officer and the incident response team notify all affected individuals and develop remediation strategies as appropriate and sufficient to the situation.

5.2.7 Manage the Incident Resolution and Aftermath

The information security officer and the incident response team will continue to update and communicate response status, determine next steps, and develop a postmortem plan to review the efficiency and effectiveness of the response and develop future prevention and/or mitigation processes and procedures.

6 FERPA COMPLIANCE

Canvas was built to comply with the Family Educational Rights and Privacy Act (FERPA) by design and Canvas readily integrates with other campus systems to prevent unauthorized access to FERPA-protected data. Whether implemented as a standalone system or as a fully integrated component of the campus IT/IS infrastructure, Canvas provides educational institutions and agencies with multiple mechanisms and technologies to manage, enforce, and comply with the provisions of FERPA and to fulfill their responsibilities under its requirements.

6.1 FERPA Overview

FERPA is a Federal law that protects the privacy of student education records. The law applies to all schools and institutions that receive funds under the applicable program of the U.S. Department of Education. FERPA provides students, and in some instances parents, the right to inspect their education records and some ability to control the disclosure of information contained in their education records.[1]

FERPA requires educational agencies, which disclose personally identifiable information from a student's education record to other school officials, to use "reasonable methods" to insure school officials obtain access to only the education records they have legitimate educational interests in.[2]

Table 6–1 identifies key sections and requirements of the Family Educational Rights and Privacy Act (FERPA) and briefly describes how Instructure and the Canvas learning management system (LMS) comply.

Table 6–1. Key FERPA Requirements and Instructure and Canvas Compliance

Item	FERPA Section	Requirements	Comments
Instructure as a "School Official"	34 CFR§ 99.31 (1)(i)(B)	(1) Performs an institutional service or function for which the agency or institution would otherwise use employees; and(2) Under the direct control of the agency or institution with respect to the use and maintenance of education records; and(3) Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records.	Instructure is under the direct contractual control by the agency or institution with respect to the use and maintenance of education records.

[1] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
[2] 34 CFR § 99.31

Item	FERPA Section	Requirements	Comments
Agency or Institution Disclosure to Instructure as a "School Official"	34 CFR § 99.31 (a)(ii)	Education institution must use "reasonable methods" to make sure school officials have access to only education records they have legitimate educational interests in.	Provide Instructure only the information needed to serve its function. Access to educational records is dictated by course enrollment and role data provided by the institution. Access inside of a course can be further limited by groupings of students.
Requirement of Further Non-Disclosure	34 CFR § 99.33 (a)(1)	School can disclose information only on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student.	Contract with Instructure specifies that Instructure not disclose the information to any other party and otherwise in compliance with FERPA.
Permission settings within the Software	34 CFR § 99.30 (a)	Parent or eligible student shall provide a signed & dated written consent before an educational agency or institution discloses personally identifiable information from the student's educational records, except as provided in § 99.31.	Agency or institution can change the permissions settings within the software to allow for, or deny, access to certain types of users.(See below page 6)
Course Settings	Same as above	Same as above	Agency or institution can change the course settings within the software to allow certain users to access the course.(See below page 7-8)
Account Settings	Same as above	Same as above	Agency or institution can change the account settings within the software to allow only certain users to access features. (See below page 9)
Names, not potentially sensitive contact information are displayed in Canvas(security feature)	Same as above	Same as above	Canvas displays students' names in the course; however students' email addresses or phone numbers will not be displayed. Students enrolled in the same course can contact one another, but the communication will be mediated through Canvas and students' email addresses will not be disclosed.
Log off inactive users (security feature)	Same as above	Same as above	Canvas automatically logs out users after a period of inactivity.

Item	FERPA Section	Requirements	Comments
Browser Session Logout(security feature)	Same as above	Same as above	Once a browser session is closed and a new browser is opened, Canvas will require the user to login again.
Authentication Integration	Same as above	Same as above	Single-sign-on is highly encouraged. All access to the system is dictated by the Institution-controlled identity system (SAML 2.0, CAS, LDAP, Shibboleth etc.).

6.2 Customization

Under FERPA, each school must define in their annual notification who constitutes a school official and what constitutes a legitimate educational interest.[3] Because of this variation, Canvas provides settings that can be configured to conform to each school's definitions. This document describes the various Canvas settings related to FERPA, the default settings, and the changes that may be made to these settings.

6.3 Permissions

One of the main FERPA-related tools available to educational agencies is the ability to define the permission settings for specific user roles in Canvas. Roles are established and communicated within Canvas by the type of course or section enrollment. The management of enrollments and the associated role permissions enable schools to specify what data each user can view. Both instructor and teacher's assistant enrollments can be limited to student data in a section, which is a sub-group of the overall course enrollments. Enrollment data is typically furnished via integration with the institution's student information system (SIS). The default permission settings can be changed to either allow or deny access to specific features and data.

To access the permission setting page in Canvas as shown in Figure 6–1, select "Permissions" from the dashboard's left hand menu in a Canvas course. In addition to the user roles of Students, Teachers, and Course Designers, Canvas also has the predefined roles of:

- TAs – individuals who serve as a teacher's assistants.
- Observers – individuals who have access to the course, but do not participate in the course.

[3] 34 CFR § 99.7

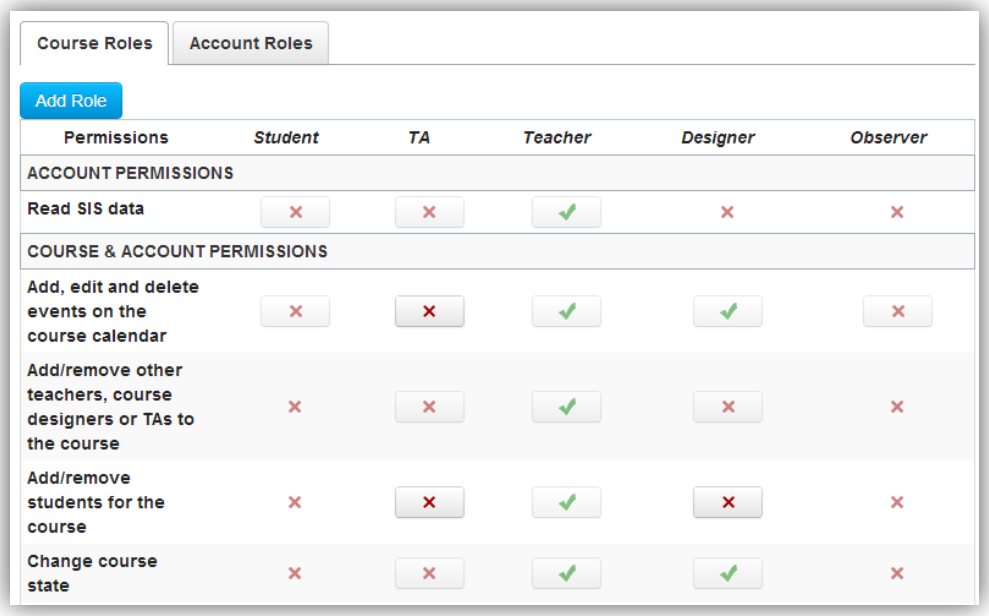

Figure 6–1. Specifying permission settings in Canvas by user group.

6.4 Course Settings

All data and course content is securely stored under an associated access control policy. Every time the data or content is accessed, this access control policy is consulted before access is granted to the requested resource. By default, Canvas only allows users enrolled in a course to view course content. With the growing need for OpenCourseWare and open educational resources, Canvas through the mechanism of these access control policies can safely permit the sharing of course content publicly while protecting and maintaining the privacy all personal and FERPA associated content. These policies support the sharing of continuously updated course content without compromising data security.

The procedures below step through the process for making a course public while keeping all the student data private and secure.

1. Click on “Courses” from the top-level navigation menu in the Canvas dashboard to display the course selection page. Select the course for which you would like to change the settings.
2. Select “Settings” from the left hand course menu to display the course details page as shown in Figure 6–2.
3. Click on the “Edit Course Details” button at the bottom of the course details page.

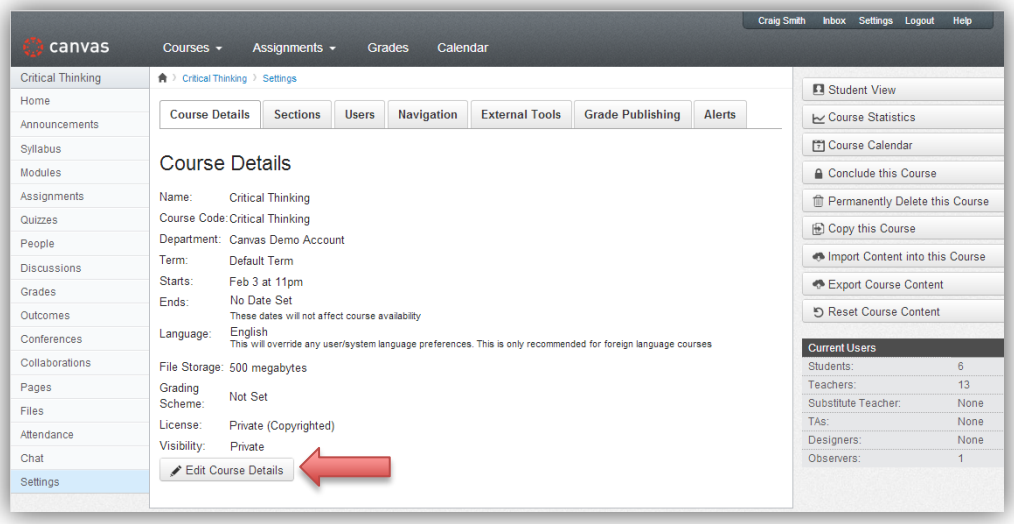

Figure 6–2. Course details page.

4. Select the box next to “Make this course publicly visible,” then click “Update Course Details” as shown in Figure 6–3.

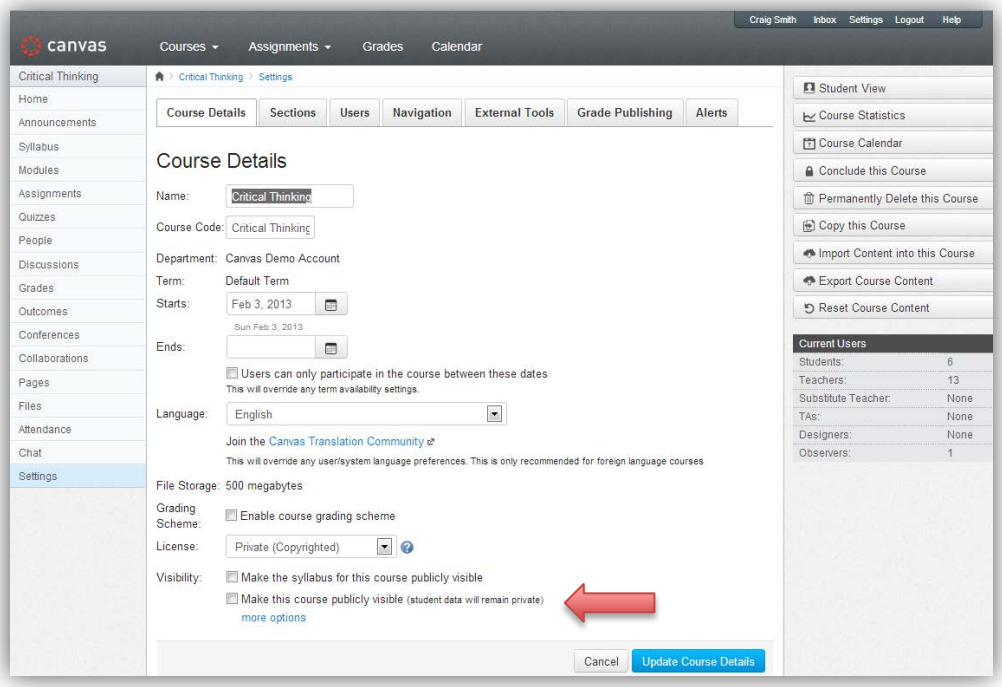

Figure 6–3. Setting the course visibility to public.

6.5 Account Settings

6.5.1 Authentication Integration

Single Sign-On (SSO) is configured at the account level. SSO gives the institution full control over which users are authenticated and how that authentication is performed. Role information is communicated with enrollment data via integration with the institution's SIS. Supported identity protocols include LDAP, Active Directory, CAS, SAML 2.0, and Shibboleth.

6.5.2 Assessment Results in External Notifications

An educational agency can decide whether or not it will allow students to have the ability to opt-in to receiving grades by external notifications through email, SMS, or other communication channels. By default, when an instructor assesses submitted assignments, students can receive notifications that they have received a grade on a specific assignment, but the notification will not include the grade received. If the educational agency has selected this option, it will allow the student to consent or opt-in to receive the grade in the notification as well.

To change the default setting:

1. Click on the "Settings" tab located on the left hand menu of the dashboard.
2. By default, the Settings tab will be displayed as shown in Figure 6–4.
3. Click on "Students can opt-in to receiving scores in email notifications" and then click "Update Settings."

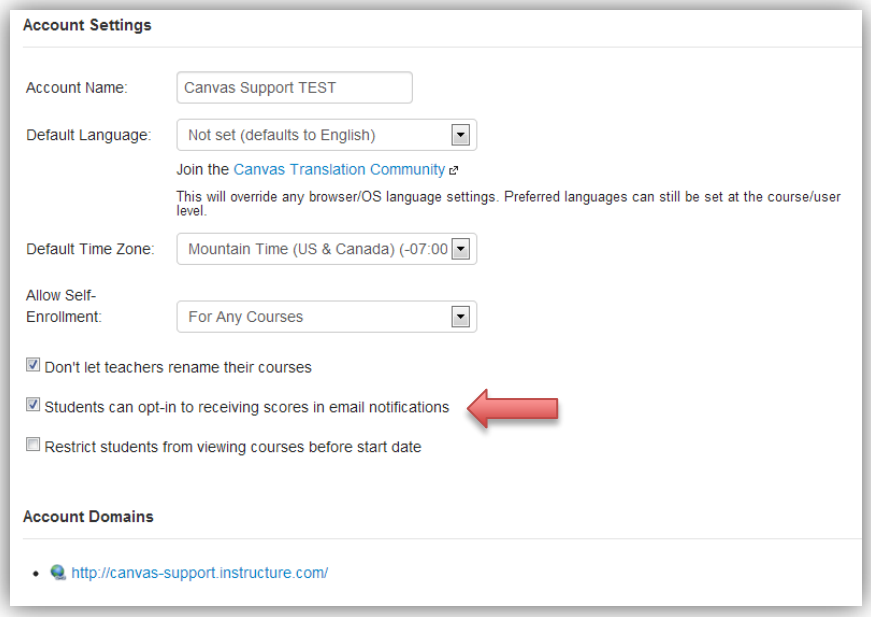

Figure 6–4. Allowing students to opt into receiving grades in notifications.

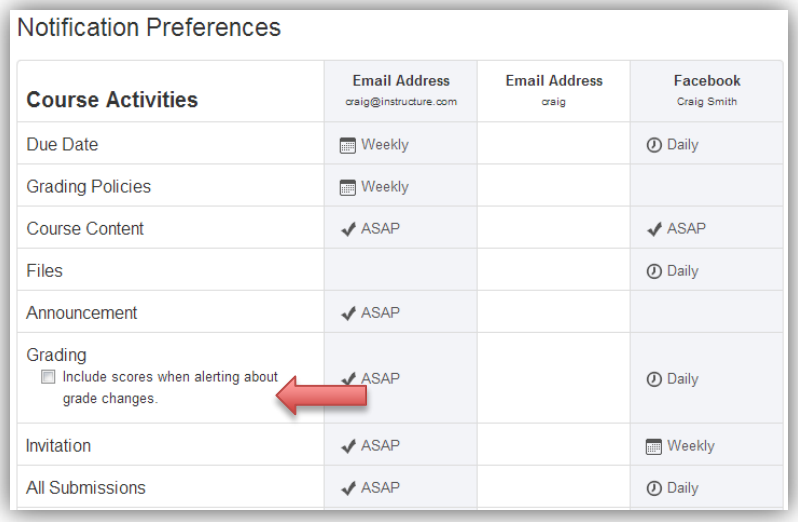

Figure 6–5. Students can opt into receiving grades notifications in their account settings.

6.6 Other Default FERPA-related Features

Additional features in Canvas related to FERPA compliance include:

- **Inactive user logout**. Canvas will automatically logout the user after a period of inactivity.
- **Browser session logout**. Once a browser session is closed and a new browser session is opened, Canvas will require the user to login again.
- **Protection of sensitive contact information**. Although Canvas displays students' names, Canvas will not display students' email addresses, phone numbers, and other sensitive contact information to other students. Canvas mediates communications, allowing users enrolled in the same course to contact one another without the disclosure of users' actual contact information. Administrators with the appropriate permissions can access the audit and record of Canvas communications.