SECURITY OVERVIEW

Engineering, Security, and Operations

June 2022

Table of Contents

INSTRUCTURE

Introduction

Overview

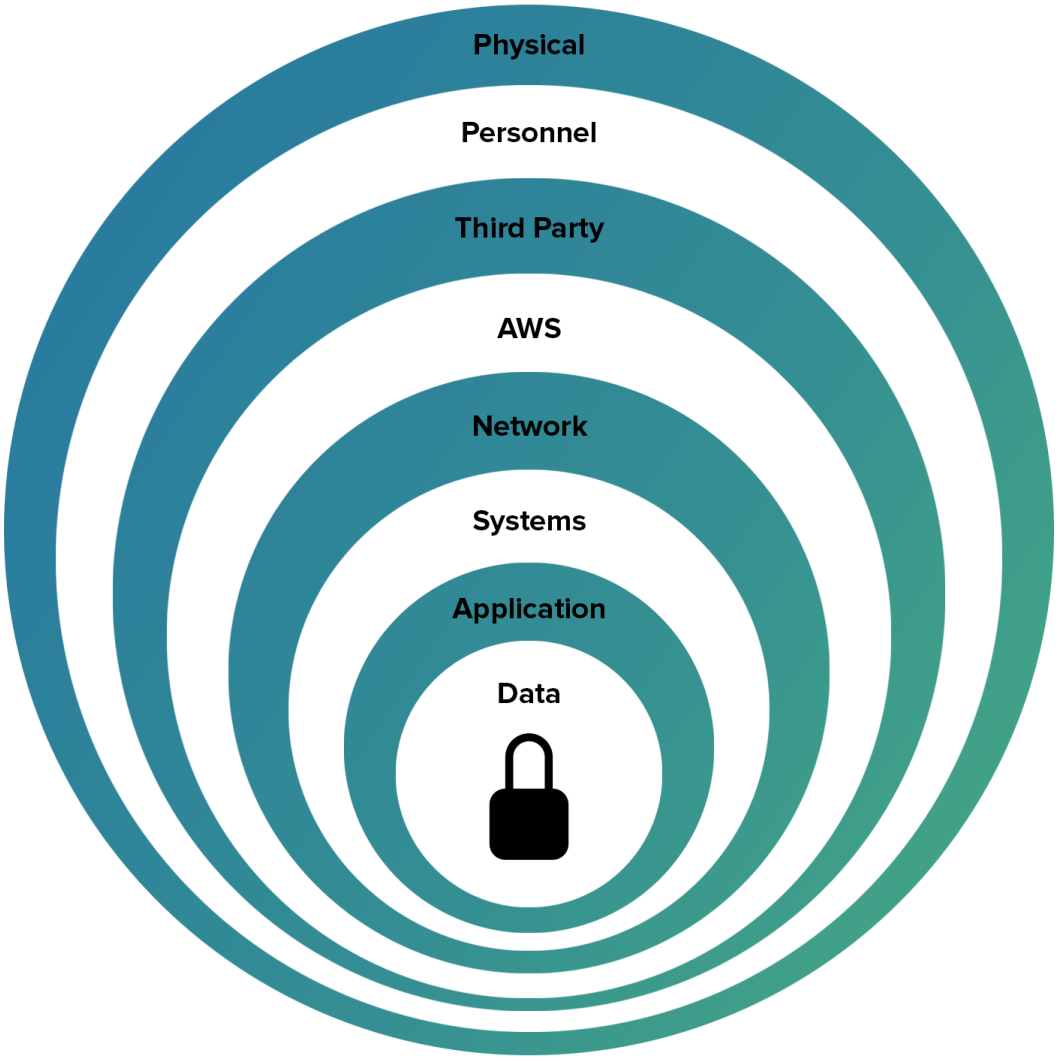
It should be no secret to anyone in today's world that security is critical. In an increasingly online world, we realize the threats to our people, our business, and your data are ever present, and the effort and measures we take to protect them is never-ending. In fact, as both our business and yours grow, we recognize the threats may also grow in severity. This past year the world has seen the rise of increasingly insidious ransomware and widespread exploits like Apache Log4j, where up to a reported 50% of all online businesses saw attempted attacks on their assets via the Log4Shell vulnerability.

This is why our security program is built based internationally-recognized standards such as ISO 27001, NIST's Cyber Security Framework, AICPA's Trust Services Principles and Criteria, and SANS' CIS Critical Security Controls. And, speaking of standards, we also ensure we develop our applications abiding with OWASP's Top 10. At Instructure, we implement both preventative and detective mechanisms, as well as processes, controls, and tools in layers—helping to mitigate risks that might impact data, people, systems, operations, products, and our mission as a company. The purpose of this document is to describe these layers and the types of controls we apply to keep our customers from badness.

Instructure's Security Program

Instructure’s security program is led by Instructure’s Chief Information Security Officer (CISO) and has a team of talented, skilled, and experienced information security professionals. Instructure’s information security team is responsible for establishing strong security practices throughout Instructure via governance, risk management, policy, education, security engineering, security compliance, security operations, and application security.

By implementing preventative and detective security mechanisms at each layer between plausible external and internal risks and Instructure’s most valuable assets, we able to enact a defense-in-depth approach to protecting customer data.



Layered Security

Physical Security

Instructure hosts all customer-facing web applications and supporting infrastructure on AWS. The AWS infrastructure is highly stable, fault-tolerant, and secure. AWS publishes an insightful security whitepaper that describes how AWS implemented physical security and environmental protection mechanisms to protect AWS data centers throughout the world. Instructure relies on AWS' ability to design and operate these critical mechanisms and controls to protect physical access to data and availability of Instructure's services.

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 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 backup power in the event of an electrical failure for critical and essential loads in the facility. Generators provide backup power for the data centers of the entire facility.

Additionally, both Canvas' and AWS' security controls have been audited by a reputable 3rd party assessment organization, and have produced the following (and many other) attestations and certifications:

- SOC 2 Type II report using the Service Organization Control framework put forth by the American Institute of Certified Public Accountants (AICPA)
- Certified ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements
- Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS) (for Canvas' Catalog product)

Personnel Security

As part of our commitment to security, Instructure is dedicated to keeping our employees up-to-date and informed of the latest industry developments and practices. Instructure provides employees with security awareness training upon hire and annually thereafter. Included as part of Instructure's security awareness training are valuable insights and guidance related to keeping customer data and Instructure assets secure from the variety of common threats against these assets. This also includes a requirement for all employees to read, understand, and sign the Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Act (COPPA) compliance forms.

Background Checks

Instructure performs background checks on all employees and contractors during the hiring process, and employment is contingent based on the results of the background check. Additional background checks such as financial/credit checks, qualification checks, criminal history, etc. are performed on key employees and/or roles, for example, employees who will be handling confidential data or holding financial roles.

Third-Party Security

Instructure utilizes several third-party organizations to host its products for customers. As part of helping ensure third-party organizations are securely providing services to Instructure, Instructure's security team performs thorough vetting prior to, and periodically throughout the relationship with third-party vendors.

To help provide reasonable security assurance of the security practices and mechanisms at these third parties, Instructure requests and reviews copies of the third-party assurance reports provided by these organizations on an ongoing basis to confirm these controls are operating effectively. Legal contracts with these third parties also include security provisions to help ensure the implementation and operation of effective security controls at the third-party organizations.

AWS Security

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

AWS Network Security

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

- **Man In the Middle (MITM) Attacks:** All AWS APIs are available via SSL- protected endpoints that provide server authentication using signed SSL certificates.
- **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 logged and investigated.
- **Virtual Private Cloud:** Instructure utilizes VPCs in order to further segment, protect, and isolate network traffic.
- **Intrusion Prevention:** Instructure uses AWS GuardDuty to alert and inform on security incidents occurring against Instructure's services hosted in AWS.
- **Intrusion Detection:** Instructure leverages Lacework on all AWS accounts, forwarding alerts to the Instructure Security Team. All output is sent to Instructure's centralized logging management system for further analysis and alert generation.

AWS Services

The AWS services used to host Instructure products include Elastic Compute Cloud (EC2), Application Load Balancing (ALB), Auto Scaling Groups (ASG), Simple Storage Service (S3), Elastic Block Store (EBS), Virtual Private Cloud (VPC), Simple Email Service (SES), Identity and Access Management (IAM), and several others. Instructure's products are designed to make full use of the real-time redundancy and capacity capabilities offered by AWS, running across multiple availability zones in regions throughout the world. Primary storage is provided by Amazon S3, which is designed for durability exceeding 99.99999999%.

AWS Regions and Data Centers

Amazon Web Services has multiple locations (called "regions") worldwide. Each region is a separate geographic area, and each region has multiple, isolated locations known as Availability Zones. Instructure uses the following Amazon Web Services (AWS) regions:

- US East (N. Virginia) Region
- US West (Oregon) Region
- Canada Central (Montreal) Region
- EU West (Ireland) Region
- EU Central (Germany) Region
- Asia Pacific (Sydney) Region
- Asia Pacific (Singapore) Region
- Asia Pacific (Mumbai) Region (*Impact product only)

AWS Data Security

Instructure has established several controls to ensure data is protected against unauthorized disclosure, modification, or destruction, including:

- All data at rest including off-site recovery backups are encrypted using the AES-GCM 256-bit algorithm.
- All data traffic in and out of Canvas is encrypted using TLS 1.2, forward-secrecy-compliant ciphers whenever possible (e.g., ECDHE-ECDSA-AES128-GCM-SHA256). The acceptable cipher list is constantly maintained to ensure that no vulnerabilities are present (e.g., CRIME, BEAST).
- Off-site recovery backups are encrypted using the AES-GCM 256-bit algorithm and stored within a highly secured location.

Additionally, data is stored redundantly in multiple availability zones through Amazon S3. Instructure products replicate data in near real-time to backup and secondary databases, and data is backed up daily. Instructure creates daily database backups of data and content to Amazon S3. Data replication and backups ensure that, in the event of a necessary system restore, the potential of data loss would be limited.

Network and Systems Security

Instructure products have 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. These products are designed to support institution's own internal security policies and to provide rigorous protection from internal or external intrusions. These products reinforce system security by presenting a simple security model to end-users.

System Access and Authentication

Instructure uses a multiple approval system for granting access to employees. 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. Other approvals are included as necessary and based on the access being requested. If all parties approve the employee's access, the respective technology 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.

Instructure's technology teams facilitate the installation of keys for all employees with access to the servers. An automated configuration system 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.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks

Instructure strictly follows industry best-practice in mitigating Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks without affecting the availability of the service to end-users. Naturally, AWS infrastructure is DDoS-resilient by design and is supported by DDoS mitigation systems that can automatically detect and filter excess traffic. For example, we employ AWS Shield as a managed Distributed Denial of Service (DDoS) protection service that safeguards the Canvas web application. AWS Shield provides always-on detection and automatic inline mitigations, and has mitigated some of the largest DDoS attacks ever recorded, stopping a 2.3 Tbps attack in mid-February 2020. This gives our customers automatic protection and defense against the most commonly occurring network and transport layer DDoS attacks. But, as is the case with our ongoing philosophy to provide a premium-tier Software-as-a-Service, we go much further than simply offering standard DDoS protection.

As a web application, the Canvas load balancers (AWS Elastic Load Balancing) only listen to a single protocol on two ports. HTTP (TCP) on port 80, which is redirected to HTTPS on port 443 which serves all data over TLS. By automatically distributing incoming application traffic across multiple targets and controlling and absorbing network traffic, the Canvas load balancers create both a highly available application for users and a robust DoS/DDoS mitigation strategy, easily deflecting malicious or unwanted requests. Reducing the attack surface in this way means we block traffic from many common DDoS attack vectors that don't communicate on the same port or protocol as our application.

By using Elastic Load Balancing (ELB), we greatly reduce the risk of overloading the application by distributing traffic across many backend instances and create a line of defense between the internet and our Virtual Private Cloud (VPC) network which hosts the Canvas service. ELB scales automatically, allowing us to manage larger volumes of unanticipated traffic, like flash crowds or DDoS attacks. The load balancers accept only well-formed TCP connections which means that many common DDoS attacks like SYN floods or UDP reflection attacks will not be accepted and passed to the application. When our load balancers detect these types of attacks, they automatically scale to absorb the additional traffic ensuring there is no change in the availability of the service to end-users.

Because the entire Canvas ecosystem runs on virtualized servers as part of Amazon Web Services (AWS) Virtual Private Clouds (VPC), we have a DDoS-resilient architecture which minimizes public entry points by way of security groups and network access control lists (ACLs). This means that not only are application attack surfaces minimized, but common DDoS attacks are quickly detected and mitigated using AWS Security Groups. We configure AWS Security Groups to allowlist (deny-all, permit-by-approved-exception) network traffic to only authorized ports, thus, automatically denying access to any other port or protocol and in turn, protecting the backend Canvas application components from a direct attack.

In addition to the above best practices, the constant logging and monitoring of the Canvas service enables us to quickly identify any legitimate DoS/DDoS attacks and engage in an immediate incident response.

Application Security

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 based on the Open Web Application Security Project (OWASP) secure coding and code review documents and other community sources on best security practices.

All developers are trained to identify and analyze security issues when writing and reviewing code. Members of Instructure's technology teams 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 Instructure products.

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

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 the following:

- 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 code branch for formal quality assurance (QA). The QA team tests the new code on all supported platforms and browsers.

Customer Identity and Access Management

Instructure's products support centralized identity management and delegated authentication via integration with Central Authentication Service (CAS) and SAML 2.0. If authentication fails, the application looks up the credentials using its internal authentication service. If authentication fails again, the application will deny the user login.

Protocol and Session Security

Instructure's products use HTTPS (HTTP over TLS) for all communication. All inbound and outbound traffic is encrypted using TLS 1.2, ensuring that all personally identifiable information, credentials exchange, page requests, and session data are secure. These products encrypt data at rest at the database layer. This includes all user information, performance, course information, and natively-built courses.

Sessions are maintained and can be invalidated. 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 be 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.

Preventing Cross-Site Scripting (XSS) Attacks

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

The applications sanitize content to protect against intentional or unintentional vulnerabilities. When content is put into a form, such as content that a user enters with the Rich Content Editor, the application scrubs (both client-side and server-side) the content and removes any malicious content. Content sanitization prevents session jacking, form hacks, and other unauthorized data access and/or modifications.

All user-inputted content is sanitized before being saved to the database. The sanitization is done by explicit allow listing--not block listing--preventing the addition of JavaScript to HTML data and prevents the addition of unsafe HTML tags as well.

File Upload and Download Security

User-uploaded files are stored in Amazon S3 with unique names and folders. To prevent side-jacking from user uploaded files and preserve the integrity of the system, Instructure's products place 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 hi-jacking. If an uploaded file executes code using JavaScript, Java, or other technologies, that code will not be able to access the user's session nor be able to make requests to the application on the user's behalf. All file downloads require unique, short-lived authorization keys.

Data Security

Instructure has an established, documented, approved, and disseminated Data Classification, Handling and Encryption Policy. This policy outlines the processes for classifying and handling data during its lifetime. As part of this policy, data are classified as one of the following:

- Confidential
- Internal
- Public

Confidential

Confidential data are sensitive data elements that legally and contractually require security and privacy protection mechanisms. Examples of confidential data include customer data, authentication information, personally identifiable information (PII), payment information, and anything subject to attorney-client privilege. Confidential data is required to be encrypted at all times both in transit and at rest, shared with only appropriate and authorized personnel, and are securely destroyed.

Internal

Internal data are data for internal Instructure use only. These data elements are considered "insider information" and are secured from the public. Examples of Internal data are email correspondence, materials marked "Instructure Internal," and other Instructure information not published or made available publicly. These data elements reside on Instructure systems and are only shared with external entities under a fully executed non-disclosure agreement (NDA).

Public

Public data is data from publicly accessible sources. Examples of public data include data from news articles, press releases, and internet searchable content. At Instructure, data classified as Public do not require any special data handling requirements.

Virus and Anti-Malware scanning

Instructure performs anti-virus and anti-malware scanning of all files uploaded and stored within Canvas that are 64MB or less in file size. Most malware typically found within files is usually less than one megabyte (MB) in size, and viruses and malware are generally not activated unless explicitly opened within Canvas. Just as with files from any other source, we recommend that academic institutions follow good security practices, such as running anti-virus/malware software and exercising due caution when running unknown files from other computers.

On all Instructure devices, we utilize enhanced endpoint detection and response (EDR) software on all devices, above and beyond standard antivirus with alert triggering.

Password Security

User passwords are encrypted. Credentials used to access the system are never stored in the application infrastructure. Rather, passwords are one-way encrypted using a combination of a random, user-specific salt value and SHA512, the cryptographic, one-way hash algorithm. Incoming credentials are passed through the same procedure and compared against the encrypted and salted stored value. In this way, Instructure has no knowledge of or way to retrieve user credentials. If a customer integrates with an external identity provider (e.g., LDAP, AD, CAS, SAML, etc.) then security settings, such as password policies, defined in the external authentication provider will be used.

As an extra layer of password security, Canvas provides built-in multi-factor authentication (MFA) functionality which can be enabled with one of three options: required for admins, required for all users, or optional for all users. Canvas' multi-factor authentication requires a mobile device in order to set up MFA with a user account. The device must be able to send text (SMS) messages, or if your users have a smartphone, they can download their preferred MFA application such as Google Authenticator or Authy, etc.

Ransomware

Instructure's robust information security program runs on a continuous, PDCA-improvement cycle. To mitigate malware and ransomware, we utilize a number of security practices as recommended by the United States Cybersecurity and Infrastructure Security Agency (CISA).

These practices include (but are not limited to):

- **Keeping systems up to date**; Removing end-of-life operating systems and libraries and keeping systems and applications updated with security patches.
- **User Management**; Provisioning users with least privilege and role-based access control. Performing regular user access reviews on all systems and directories, specifically prohibiting shared accounts.
- **User endpoint security**; Utilizing enhanced endpoint detection and response (EDR) software on all user devices, above and beyond standard antivirus.
- **Multi-Factor-Authentication**; Enabling multi-factor-authentication in front of all VPNs, bastions, and applications to prevent the reuse of any lost credentials. Logging and alerts on new and unusual IPs and locations used by a user to authenticate to services.
- **Disaster Recovery**; A comprehensive disaster recovery plan that identifies the critical components of each service and how each critical component is backed up and recovered in response to a significant event. The recovery of each critical component is regularly tested.
- **Data mapping**; Auditing sensitive data storage. Reducing elements of stored data to only what is necessary to operate a service. Ongoing reviews and monitoring on systems with sensitive data storage.
- **DevOps**; All code goes through developer peer-review before it is merged into the code base repository and is scanned for security vulnerabilities (including dependencies) before release to production.
- **Vulnerability Identification**; Public facing endpoints and internal environments are scanned for vulnerabilities on a regular basis. Competent third parties are engaged for targeted penetration testing to discover security issues. Crowd-sourced security testing is encouraged and rewarded.
- **Simplify and Optimize**; We implement a common set of security controls across all teams and services. This includes a consistent method of user authentication to servers, cloud environments and production services.

- **Security Team**; A dedicated security team with the overall responsibility of security residing within the organization. The security team is responsible for all aspects of security being accounted for in communication to management, risk analysis, and quarterly and yearly planning to incorporate security work for all teams.

- **Training**; Ongoing and regular staff security training including, but not limited to, automated phish testing of all staff and remediation of phish-prone staff.

Vulnerability Management and Security Audits

Internal Security Reviews and Vulnerability Management

Instructure's security team conducts vulnerability scans of the production environment and annual third-party code base and penetration testing. 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. In these audits, the security team:

- Scans the application externally, using both off-the-shelf and custom internally built 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.

External Security Reviews

In addition to our frequent internal security audits conducted throughout the year, Instructure conducts annual, open, third-party security reviews. The open, external security audit is one way that Instructure can demonstrate not only the state of application security, but also our responsiveness to any vulnerabilities. Instructure issues security vulnerabilities to our customers, and because Instructure's products are multi-tenant applications, 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 customers who are interested in conducting their own security audit of Instructure's products, Instructure will, upon request, set up an environment where they can conduct automated and manual vulnerability scanning.

SOC 2 Compliance

Instructure produces, on an annual basis, SOC2 Type II reports for our products which cover the following principles: Security, Availability, Confidentiality, Processing Integrity, and Privacy. These reports are available under mutual NDA.

ISO 27001 Compliance

Instructure is certified as ISO 27001:2013 compliant for products including Canvas LMS, Canvas Studio, Canvas Student Pathways (formerly Portfolium Pathways), Canvas Student ePortfolios (formerly Portfolium ePortfolios), and Mastery Connect.

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, Instructure's products are cloud services 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 applications and infrastructure are conducted using third-party tools, 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 production environments.

Instructure, in coordination with AWS, takes a proactive approach to enforcing SOC 2 controls. Retrospectives are completed after any significant operational issue, regardless of external impact, and retrospective (root cause analysis) 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.

Incident Response Policy and Plan

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. Instructure realizes that no organization is impenetrable and, accordingly, prepares plans to help most effectively facilitate a security incident.

Incident Response Policy

Backing up these preventative measures, Instructure has established a set of prescriptive responses to be executed in the event of unauthorized access to systems or unauthorized data exposure. Unauthorized access occurs when an unauthorized person (e.g., a bad actor, or malicious employee) gains access to Instructure systems via exploitation of a system vulnerability or social engineering. 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 Incident Response policy has been designed to ensure:

- Earliest possible detection of a system or data security breach; through both manual and automated detection methods
- Rapid securing of the system and data to prevent further unauthorized exposure
- Responsive notification to users and other affected parties that unauthorized access may have been granted and/or confidential or personal information may have been or was exposed or compromised by a breach in system security.

Incident Response Plan

In the event of a breach of security and potential unauthorized data exposure, Instructure's Chief Information Security Officer (CISO) 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.

Determine the Scope of the Security Breach

In all cases, Instructure's CISO 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, Instructure's CISO 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.

Assemble the Incident Response Team

Instructure's CISO will assemble the incident response team. The composition and charge of the team will depend upon the type of breach and resulting data exposure. The team conducts a preliminary assessment to help develop a tailored response. Once the incident is contained, this team will also evaluate changes in processes, systems and/or policies to prevent a repeat event.

Control Dissemination of Information

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

Alert Executive Team

Instructure's CISO will alert the appropriate senior administrators including the Instructure executive team, client institution officials, system engineers, and other key players as warranted.

Identify Affected Persons

Instructure's CISO will work with institution officials, including Instructure's SVP of Engineering and Instructure's VP of Operations, and the incident response team to determine the identities of affected individuals and determine the extent of the data exposure.

Notify Impacted Organizations

Instructure's CISO will work with the SVP of Engineering, General Counsel, VP 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 forty-eight (48) hours. These legal requirements will vary on a state-by-state basis. Working with the appropriate parties, Instructure's CISO and the incident response team notify all affected individuals and develop remediation strategies as appropriate and sufficient to the situation.

Manage the Incident Resolution and Aftermath

Instructure's CISO 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.

FERPA/HIPAA Compliance

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.

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

Instructure products are built to comply with the Family Educational Rights and Privacy Act (FERPA) by design, and they readily integrate 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, our products provide 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.

FERPA Enforcement

Each user has a unique portal based on their role. Canvas offers roles and permissions that allow administrators to have a large degree of control over what information each role has access to. User's, based on their successful authentication and designated role, will only have access to the content as designed by the end customer. In order to maintain compliance with FERPA regulations, Canvas will give customer all the tools it needs to maintain its FERPA compliance. Examples of FERPA compliant features include:

- Canvas allows access to student information only to those to whom permission is granted. By default, that is the administrator for the Institution's Canvas instance and faculty who are teaching courses in which the student is enrolled. It is possible to grant permission to others identified by the institution as "School Officials" (as described in FERPA guidelines), or to remove permission from either administrators or faculty. In short, the institution is in full control.

- All access to Canvas is encrypted. There are no exceptions. When transmitting SIS data, the information is safe in transit and, when it arrives in the Canvas system, it is protected by the same account and role-based permissions that secure all other data.

Note: It must be stressed that FERPA is the customer's responsibility: they own the data and they are in full control of all access to it. As long as customers follow Canvas best practices then private information will remain private in Canvas.

HIPAA Overview

Canvas is not HIPAA compliant. HIPAA compliance has not been made a core product initiative, as Canvas is used in the educational environment and is not intended to store health information. As such, we are unable to sign any Business Associate Agreements (BAA).

Payment Card Industry ("PCI") Data Security Standards (“DSS”).

As an LMS, Canvas does not store, process, or transmit credit card data, and as such is not required to adhere to PCI DSS.

Our Canvas Catalog product redirects users to integrated payment gateways set up by the client institution. Catalog is compliant with PCI DSS as demonstrated by Instructure's self-assessment questionnaire (SAQ) form D. This SAQ is available upon request and execution of a non-disclosure agreement.

General Data Protection Regulation (GDPR)

GDPR stands for the EU General Data Protection Regulation. The GDPR is a European Union (“EU”) law that regulates the personal data of individuals in the EU. The GDPR harmonized data protection law across the EU and introduced sweeping changes that require companies to make significant updates to their privacy and security policies and practices. Instructure is committed to helping our customers comply with GDPR.

Instructure has complied with the GDPR since the enforcement date (25 May 2018).

To ensure ongoing compliance with the GDPR, Instructure does the following:

- Educates the organization about GDPR and its requirements.
- Has conducted a GDPR gap analysis with the help of a reputable outside law firm experienced with GDPR and has closed those gaps.
- Maintains an up-to-date listing of personal data Instructure holds, where it came from, and who Instructure may share it with.
- Maintains current privacy notices that comply with the GDPR.
- Ensures existing procedures cover all the rights individuals have under GDPR.
- Identifies our lawful basis for processing personal data, documenting it, and updating our privacy notice to explain it to individuals.

- Reviews how Instructure obtains, records, and manages consent.
- Reviews and updates contracts with third parties to ensure our privacy obligations are up to date.
- Ensures the right procedures are in place to detect, report, and investigate a personal data breach.
- Maintains processes for Data Protection Impact Assessments.
- Has appointed a Data Protection Officer.

Safeguards for Cross-Border Data Transfer

One of the GDPR's requirements is that any personal data transferred "cross-border", i.e., outside of the EU, can only be moved pursuant to a legal mechanism.

Instructure uses the European Commission's Standard Contractual Clauses (model clauses) as a lawful method to transfer personal data outside the EU. By incorporating the model clauses into Instructure's Data Processing Addendum ("DPA"), both data controllers (Instructure's EU-based customers) and data processors (Instructure) are contractually obligated to certain technical and organizational safeguards relating to individuals' (Instructure's EU-based customers' end users) privacy rights.

Conclusion

We realize security is paramount for our customers in a SaaS-driven world. That's why we take extreme care to implement both preventative and detective mechanisms, as well as processes, controls, and tools in layers—helping to mitigate risks that might impact data, people, systems, operations, products, and our mission as a company. As outlined in this document, our dedicated security team is full of passionate, skilled, and experienced security professionals, who, along with ensuring compliance to third-party assessment such as the Service Organization Control framework, focus on detecting and protecting against badness, and earning and maintaining your trust.