Proprietary & Confidential

MASTERY
BY INSTRUCTURE

MasteryConnect System

SOC 3

Relevant to Security, Availability, Confidentiality, and Privacy

JULY 1, 2022 TO JUNE 30, 2023

MOSSADAMS

Table of Contents

I. Independent Service Auditor's Report

Instructure, Inc.
6330 South 3000 East, Suite 700
Salt Lake City, UT 84121

To the Management of Instructure:

Scope

We have examined Instructure's accompanying assertion in Section II titled "Instructure's Assertion" (assertion) that the controls within Instructure's MasteryConnect System (system) were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Instructure's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Instructure uses Amazon Web Services for hosting services (subservice organization). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Instructure, to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Instructure's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Instructure, to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Instructure is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Instructure's service commitments and system requirements were achieved. Instructure has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Instructure is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Instructure's service commitments and system requirements based the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Instructure's MasteryConnect System were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Instructure's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Moss Adams LLP

Salt Lake City, Utah
October 4, 2023

II. Instructure's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Instructure's MasteryConnect System (system) throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that Instructure's service commitments and system requirements relevant to Security, Availability, Confidentiality, and Privacy were achieved. Our description of the boundaries of the system is presented in Section III titled "Instructure's Description of the Boundaries of Its MasteryConnect System" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Instructure's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP Section 100*, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Criteria)*. Instructure's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III titled "Instructure's Description of the Boundaries of Its MasteryConnect System".

Instructure uses Amazon Web Services for hosting services (subservice organization). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Instructure, to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Instructure's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Instructure, to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria. The description presents Instructure's complementary user entity controls assumed in the design of Instructure's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Instructure's service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Instructure's Description of the Boundaries of Its MasteryConnect System

A. System Overview

1. Services Provided

COMPANY OVERVIEW

Instructure is focused on helping institutions improve education through technology. Instructure's workforce includes over 1,000 professionals and is publicly traded. Instructure provides the MasteryConnect System (MasteryConnect), wherein teachers can administer assessments and immediately see student mastery levels of key learning standards in an intuitive, visual way.

Instructure was incorporated in September 2008, and is headquartered in Salt Lake City, Utah.

SYSTEM DESCRIPTION

Key features, services, and strategies that differentiate MasteryConnect include:

MasteryConnect is the assessment and curriculum platform that transforms assessment and data cultures in schools and districts by empowering educators to move past simply collecting data to using standards-based data to directly impact teaching and learning in real time.

Instructure's MasteryConnect houses more than one million preloaded standards, so educators can immediately measure students' levels of understanding in an intuitive, visual way. The flexible teacher-centric assessment and data analysis features drive more meaningful, instructional practice and professional learning community (PLC) collaboration, while providing teachers with the insight they need to deliver a personalized learning experience for every student. After assessments are administered, the powerful MasteryConnect reporting suite makes handling the resulting standards-based data more manageable, shareable, and—most importantly—actionable.

As a standards-based assessment system, MasteryConnect was designed to link the elements of instruction, assessment, and reporting with a major focus on creating context for the use of data. MasteryConnect allows for the implementation of the Backwards Design model starting with the standards, creating structure around those standards, and aligning resources around the standards at the teacher, school, district, or state level. This model allows instructors to plan lessons and courses with a focus on student learning.

MasteryConnect teacher and district tools make each step of the teaching and learning cycle more efficient:

- Planning tools streamline the development of curriculum and assessment maps at the state, school, or teacher level. Educators can easily access national, state, and local standards, and content. The maps can be shared with selected users or automatically distributed to a Mastery Tracker from the curriculum map, which provides access to a common set of guaranteed and reliable curriculum and assessment resources.

- Synchronized curriculum maps define scope and sequence, while providing an easy way to make updates and additions to curriculum that are immediately available to teachers. This functionality allows for an organic approach to developing and refining the structure and content of the maps.
- Assessment and data are the foundation of the platform. The system includes teacher-centric formative and interim assessment tools. With these tools, teachers can easily create standard-aligned assessments using vetted item banks, district-created item banks, or more traditional authoring tools (i.e., Word, Google, text editors). Teachers have access to an online community of teacher-created, standard-aligned assessments, which number in the hundreds of thousands.
- Playlists deliver standard-aligned resources in organized playlists, which can be distributed directly to the students to help guide remediation and offer further enrichment opportunities. Teachers then identify standards in an intervention and target playlists directly for students.
- Reporting in MasteryConnect is centered on the context in which the data reports are used. MasteryConnect provides numerous methods for reporting and evaluating data to stakeholders in a way that they can use the data. Upon completion of an assessment, data is immediately available and disaggregated by standard within teachers' Mastery Tracker, enabling them to quickly identify students' levels of understanding and determine next steps.

Teachers also have access to an analysis of the item and overall results, which can be compared directly to other teachers within their school. Custom reports allow for a deeper analysis of the data using demographic indicators. MasteryConnect also allows teachers to immediately do a side-by-side comparison of their formative data to their interim assessment data.

SYSTEM BOUNDARIES

The system boundaries for consideration within the scope of this report are the processes, infrastructure, and software that store, access, operate, or transmit user data within MasteryConnect. Specifically, the system environment includes the production systems, network, and workstations, as well as the personnel who support the system for MasteryConnect.

Excluded from the scope of this report are other Instructure products such as Canvas, Studio, Catalog, Canvas Credentials, and Elevate.

SUBSERVICE ORGANIZATIONS

Instructure utilizes Amazon Web Services (AWS) to support the Instructure MasteryConnect systems. AWS provides a secure IT infrastructure for compute power, storage, and other application services over the internet. Authentication controls to the AWS administrator console are controlled by the AWS Identity and Access Management (IAM) tools.

This subservice organization is excluded from the scope of this report; the controls it is expected to provide are included in the subsequent section titled *Complementary Subservice Organization Controls.*

2. Infrastructure

Instructure's production computing, storage, and networking infrastructure is hosted on the AWS public cloud service. The infrastructure is distributed across discrete regions and availability zones within the AWS enterprise. This solution allows for the quick creation or destruction of compute, storage, and network resources based on customer demand with minimal budget impact or lead time. Instructure utilizes the following AWS services to facilitate the operation of MasteryConnect:

AWS Service	Function
Elastic Compute Cloud (EC2)	Provides a virtual computing environment that uses web service interfaces to perform the following functions: • Launch instances of operating systems. • Create Amazon Machine Images (AMIs) containing applications, libraries, data, and associated configuration settings. Configure security and network access on the Amazon EC2 instances.
CloudWatch	Provides monitoring for AWS cloud resources and applications. Amazon CloudWatch provides visibility into resource utilization, operational performance, and overall demand patterns—including metrics such as central processing unit (CPU) utilization, disk reads and writes, and network traffic. Amazon CloudWatch provides the ability to review statistics, view graphs, and set alarms for specified metric data.
CloudTrail	CloudTrail is an AWS service that helps enable operational and risk auditing, governance, and compliance of an AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.
Elastic Block Store (EBS)	EBS provides raw block-level storage that can be attached to EC2 instances and is used by Amazon Relational Database Service.
Relational Database Service (RDS)	RDS is a web service used to operate relational databases in the AWS cloud.
Simple Storage Service (S3)	Object storage used in conjunction with Amazon ECS to store object data.
Virtual Private Cloud (VPC)	Used to provision logically isolated virtual networks in the AWS Cloud. Amazon VPC is used to manage the virtual networking environment, including selection of Internet Protocol (IP) address ranges, creation of subnets, and configuration of route tables and network gateways.

3. Software

Instructure builds and delivers MasteryConnect as a Software as a Service (SaaS) offering. Each customer has a compartmentalized instance of the application, which is administered and customized by the customer using back-office functionality.

In addition, Instructure leverages the following tools:

- Okta as an authentication service
- GitHub as a code management tool
- Lacework and CloudTrail as monitoring utilities

4. People

People consist of the personnel involved in the development, operation, and use of a system (including developers, operators, users, and managers). The following outlines the various teams and functions that support MasteryConnect:

- *Customer Success* – This team is responsible for managing customer accounts and communicating directly with clients.
- *Customer Support* – This team is responsible for responding to and resolution of customer request tickets from end users and administrators at institutions. The Customer Support team is separated into multiple levels, including L1, L2, and L3 support representatives, who handle ticket flow. Any ticket unable to be resolved by this team is routed to the Engineering team.
- *Engineering* – This team is responsible for building and maintaining MasteryConnect, including new feature development, maintaining current products, updating code, and fixing bugs.
- *Human Resources (HR)* – This team is responsible for hiring, benefits design and administration, employee relations, personnel growth, and performance evaluations through regular employee check ins, and overall compliance. HR also oversees the office administration and facilities staff.
- *Information Technology (IT)* – This team is responsible for supporting and assisting the maintenance of personal computer systems, databases, firewalls, Active Directory, networks, telephones, copiers, and general computer and network troubleshooting at Instructure.
- *IT Operations* – This team is responsible for designing, automating, and maintaining a large systems environment to support MasteryConnect. This team's activities include automation, configuration management, writing code, and managing scale while effectively spinning up servers to maintain a highly available application for customers.
- *Legal* – This team is responsible for fielding whistleblower submissions and privacy inquiries. This team is also referred to as the Privacy team.
- *Product* – This team is responsible to steer the features, enhancements, and user experience for MasteryConnect. The Product team also develops new ideas and features based on industry understanding. This team maintains direct contact with customers, prospects, and market trends.
- *Security* – This team is responsible for the security of each layer of the technology stack supporting MasteryConnect — including physical, personnel, network, AWS, systems, application, code, and data.
- *Senior Management* – This team is responsible for oversight of company operations. All other teams report up to the Senior Management team.
- *Technology Leadership* – This team is responsible for meeting monthly to discuss technological needs of Instructure products. The team includes leadership from the Security and Engineering teams.

5. Data

MasteryConnect stores the following credential, profile, and transaction data on behalf of institutions and their users:

- Credential data consists of username, password, and multi-factor authentication (MFA) questions and answers used to protect user transaction data. These credentials are stored in a one-way, salted hash format.
- Profile data consists of user demographic data, including name, email, age, and gender.
- Transaction data consists of data gathered and curated during the course of users utilizing the features and functions of the MasteryConnect web applications.

6. Processes and Procedures

The following is a list of Instructure's policies and a description of the contents contained within each policy:

- *Asset Management Policy* – Instructure maintains policies and procedures to help ensure assets, including servers, workstations, software, network devices, and media containing customer data, are managed from the point of acquisition to the point of decommissioning.
- *Customer Support Policy* – Instructure maintains policies and procedures for the Customer Support team to provide guidance on support protocol, including the appropriate use of client data.
- *Data Classification, Handling, and Encryption Policy* – Instructure maintains policies and procedures to help ensure customer and internal data are properly treated and protected according to their classification. The policy includes access rights, access restrictions, data retention, and data destruction requirements.
- *Disaster Recovery Plan* – Instructure maintains documented procedures to be followed in the event a disaster or other event threatens the availability of Instructure's products.
- *Disaster Recovery Policy* – Instructure maintains policies and procedures for addressing natural disasters, environmental hazards, and other incidents that would impair system functionality or cause accidental data disclosure.
- *End-User IT Security Policy* – Instructure maintains policies and procedures to help ensure devices are accessible only by internal employees and to prevent unauthorized access to company sites and equipment.
- *Incident Response Plan* – Instructure maintains documented procedures to be followed in the event of a disaster.
- *Enterprise IT Security Policy* – Instructure maintains policies and procedures for general information security which includes roles and responsibilities supporting Instructure's service commitments and system requirements.
- *Logging Policy* – Instructure maintains policies and procedures to govern the logging of system and application events, which include types of events logged, where logs are stored, and for how long.
- *Logical Access Policy* – Instructure maintains policies and procedures to help ensure processes are in place for managing access to systems by identifying users, authenticating users, and appropriately authorizing and provisioning user access to systems.

- *Network Security Policy* – Instructure maintains policies and procedures to help ensure firewalls are configured to limit network traffic to only approved ports, keeping network devices secured and up to date, configuring remote access for secure authentication, configuring wireless networks, and using effective intrusion detection technology.
- *Password Policy* – Instructure maintains policies and procedures to help ensure its personnel manage passwords using secure creation and handling.
- *Prime Directive* – This directive provides guidance to the Customer Support team concerning how to help end users change and access their own personal information.
- *Risk Management Policy* – Instructure maintains policies and procedures that define risk tolerances and include the identification, analysis, communication, and mitigation of risks relating to company operations, information technology, safeguarding of informational assets, product development, and changes in regulatory requirements or business relationships.
- *Security Awareness Policy* – Instructure maintains policies and procedures to provide its personnel with security training as part of onboarding and annually thereafter.
- *Security Incident Response Policy* – Instructure maintains policies and procedures to help ensure its personnel prepare, identify, and contain security, confidentiality, and privacy incidents. The policy also includes definition of responsibilities, escalation procedures, and notification requirements.
- *Software Development and Change Management Policy* – Instructure maintains policies and procedures for changes deployed to production environments, which include code changes, system configuration changes, architecture changes, and any other changes that would impact the security, availability, confidentiality, and privacy of production environments.
- *Third-Party Security Policy* – Instructure maintains policies and procedures to assess and monitor the security compliance of its critical third-party service providers.
- *Vulnerability Management Policy* – Instructure maintains policies and procedures that define how its personnel continuously identify, assess, and mitigate vulnerabilities based on overall risk rating.
- *Whistleblower Policy* – Instructure maintains policies and procedures to provide communication for ethics concerns.

AUTHENTICATION

Employees utilize unique user IDs to authenticate to systems, and policy prohibits users from directly authenticating using service accounts. Access to the internal systems requires a valid username, MFA token, and password to authenticate. In addition, password authentication systems are configured to perform the following:

- prevent the reuse of at least the last 12 passwords
- restrict the use of 3 or more repeating characters
- restrict the use of a password that contains a user's display name or username
- check a user's proposed password against a blacklist of known weak passwords and dictionary words
- limit authentication attempts to 5 times prior to account lockout for 60 minutes

Authentication to the AWS Admin Console requires multiple factors (valid username and password, and one-time passcode). The AWS environment enforces a minimum password length of 12 characters and prevents the reuse of the most recent 24 passwords. The application requires a minimum password length of eight characters, or end users can tie in their existing single sign-on solution.

USER ACCESS ADMINISTRATION

Administrative access to production databases is restricted to the Engineering team through role-based access.

New and modified access for internal personnel requires documented manager approval prior to these personnel receiving access. Additionally, the Security team performs a quarterly access review to validate ongoing appropriateness of access for internal Instructure employees and contractors within the production systems and databases. The IT and IT Operations teams disable or remove the relevant user accounts within five business days of termination.

MasteryConnect end users are provisioned accounts through their respective local administrator. Local administrator accounts are provisioned for the user entity when the MasteryConnect instance is first set up.

NETWORK SECURITY

Instructure utilizes asset tags to classify infrastructure components. Tags help manage, identify, organize, search for, and filter AWS resources.

Secure communication protocols are utilized to protect information transmitted over the internet. The storage of information, including user authentication information, and the transmission of private or confidential information through MasteryConnect is encrypted using Transport Layer Security (TLS) over Hypertext Transfer Protocol Secure (HTTPS) connections. Additionally, external connections to internal production systems pass through a firewall, limiting traffic to approved ports in accordance with the Network Security Policy.

ENCRYPTION

Communications with Instructure systems over public networks are encrypted using TLS 1.2 or higher. Data is encrypted at rest in production and non-production customer environments.

VULNERABILITY MANAGEMENT

To validate application layer security, vulnerability scanning occurs monthly to validate that internal and public-facing systems are secure. In addition, the Security team engages a third party to either perform a penetration test or conduct researcher-based testing (i.e., a bug bounty program) for Instructure's client-facing services. Critical and high severity vulnerabilities are tracked to remediation.

ENDPOINT MANAGEMENT

The Instructure IT team manages the configuration of desktops and laptops used by employees. Laptop and desktop computers are configured with full hard drive encryption and anti-malware software. The IT team centrally manages the anti-malware software to help ensure computers are periodically scanned and have updated signatures.

INCIDENT MANAGEMENT

Intrusion Detection Systems (IDS) monitor traffic at internet borders. The Security team uses IDS to identify, monitor, and evaluate security threats and unusual system activity. Alerts for these events are sent to the Security team and tracked to resolution.

Management has established a Security Incident Response Policy outlining the process of identifying, prioritizing, communicating, assigning, and tracking incidents through to resolution. Security events and incidents are documented and evaluated in a ticketing system through to resolution in accordance with the Security Incident Response Policy. The Security team communicates incidents internally and externally. Incident details such as analysis, rating, impact, and resolution are documented.

The Security team tests the Incident Response Plan annually, via simulation or retrospective of an actual event. Lessons learned are incorporated into the plan.

CHANGE MANAGEMENT

MasteryConnect is continually updated to meet user needs and to enhance both the functionality and the security of MasteryConnect. Instructure employs an agile application development methodology. To help ensure changes are made in a controlled manner, Instructure has implemented controls related to the documentation, testing, and migration of code into the production environment.

Code changes may be initiated via customer request or feedback, or through internal initiatives. Ticketing systems and code review tools are in place to document code changes and any required data changes from identification through the development and deployment processes. Once the requirements are defined, a member of the Engineering team develops new code in a local development environment (Instructure maintains separate development, Quality Assurance (QA), and production environments). A peer developer then reviews the code. Upon review, the new code requires a documented peer approval that serves as authorization to move the change into the staging environment to undergo testing. Branch protections enforce peer review on code and configuration changes. Access to modify branch protection settings is restricted to Engineering Managers and the IT team.

The Engineering team performs a QA review by testing application software, including code changes, through automated continuous integration (CI) scripts or manual testing. When a successful CI build has been accomplished, the code is ready to be released into production. The code is released via deploy scripts. Access to deploy changes to production environments is restricted to members of the Engineering team through role-based access.

Emergency code changes (hotfixes) follow the standardized code change process, including authorization and testing, but are released to production outside of the established release schedule.

Configuration is managed as code, and as such, the peer approval and testing process applies to configuration changes as well as code changes.

SYSTEM AVAILABILITY

Production capacity and operational processes are monitored. Alerts are communicated to the Engineering team for triage and resolution.

Instructure has implemented controls and procedures to help ensure the availability of MasteryConnect. Data backup procedures have been configured within AWS to run a daily full backup snapshot of MasteryConnect databases. Monitoring mechanisms alert the Engineering team of backup failures. Failures are tracked to resolution. MasteryConnect backups are configured to be retained for one year. Backup data restore testing is conducted at least annually to validate the integrity of backups.

Production data is replicated to provide data redundancy. Also, application servers are configured to automatically scale to customer demand.

Instructure maintains a formal disaster recovery plan. The Security and IT Operations teams test the plan at least annually through tabletop exercises.

DATA MANAGEMENT

Instructure is committed to complying with its Data Classification, Handling, and Encryption Policy and the commitments made in the Terms of Service and Product Privacy Notice. Instructure retains and destroys customer data according to the Data Classification, Handling and Encryption Policy. Client data is retained for the duration the customer utilizes MasteryConnect. Customers may request the removal of their data. Requests from individuals or institutions to delete data are tracked via the internal ticketing system until the requested data is securely deleted. If the request is denied, the data subject is informed of the denial and informed of the reason for such denial.

Additionally, data validation checks are in place within MasteryConnect to validate the completeness, integrity, timeliness, and authorization of the data received into the company environment. Errors from data inputs are returned to the end user to re-enter the data in the correct format.

PRIVACY

Instructure provides the Instructure Product Privacy Notice publicly on Instructure websites. Instructure's Product Privacy Notice is included in the footer of Instructure's public-facing websites, as well as the Canvas application. The Product Privacy Notice includes provisions related to regional privacy law requirements including the US, European Union, Brazil, and the Australia-Pacific region.

Instructure's Product Privacy Notice also includes provisions for:

- Purpose for collecting personal information
- Choice and consent
- Types of personal information
- Methods of collection
- Use, retention, and disposal
- Access

- Disclosure to third parties
- Security for privacy
- Quality, including customer responsibilities for quality
- Monitoring and enforcement

Instructure collects and uses personal information only to the limit allowable as outlined in the Product Privacy Notice by enforcing data elements collected at the application layer and backend database.

Instructure executes contractual commitments with vendors or third parties with access to personal information. These contracts require that vendors or third parties (a) comply with applicable data privacy laws world-wide related to the processing of personal information, (b) maintain appropriate administrative, technical, and operational controls related to the processing of personal information, (c) notify Instructure of any event that impacts the integrity, security, confidentiality, or privacy of personal information, (d) notify Instructure of an unauthorized use or disclosure of personal information, (e) provide Instructure audit rights for privacy and security controls, (f) comply with data subject access requests as required by Instructure, (g) notify Instructure of any third parties that process personal information, (h) only process personal information as described in the applicable services contract or data processing agreement, and (i) not transfer personal data to any unapproved regions.

Access to personal information is recorded in web application logs. Instructure's Customer Support team provides access to a data subject's personal data processed by Instructure and can provide a data extract of such personal data upon request by the data subject with approval by the applicable customer. If Instructure is unable to provide a copy of the requested personal information processing activities, either (a) Instructure's Customer Support team informs a data subject if their access request has been denied, or (b) Privacy team provides notification, or (c) Customer Support team refers the data subject back to their institution. End users are able to access or make corrections to their private data through the application.

Instructure's methods for collecting and processing personal information are reviewed at least annually to ensure those methods of collection are completed lawfully, and fairly. This review is completed by reviewing (a) internal privacy impact assessments, (b) vendor and third-party assessments, and or (c) internal personal data inventories.

Instructure's Vendor Data Processing Agreement requires that vendors or other third parties with access to personal information notify Instructure in the event of actual or suspected unauthorized disclosures of personal information. Incident notifications are sent to Instructure's CISPO and evaluated in accordance with Instructure's Incident Response Policy.

The Instructure Legal team notifies customers (institutions) of material changes to the Instructure Product Privacy Notice via email. End users are notified via the "Global Announcements" function in the application.

B. Principal Service Commitments and System Requirements

Instructure designs its processes and procedures to provide a secure environment for customer data. Instructure's security, availability, confidentiality, and privacy commitments and system requirements are documented and communicated to customers in the Terms and Conditions, and at other resources listed below:

- Trust Center (https://www.instructure.com/trust-center)
- Instructure's Product Privacy Notice (https://www.instructure.com/policies/privacy)

Instructure's service commitments include, but are not limited to, the following:

- Data retention for at least 90 days after client termination
- Security training upon hire and annually thereafter
- Restricted logical access and strong authentication requirements
- Security threat monitoring
- Encryption in transit using TLS 1.2 or higher
- Encryption at rest
- Compliance with the EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework

C. Complementary Subservice Organization Controls

Instructure's controls related to the MasteryConnect System cover only a portion of overall internal control for each user entity of Instructure. It is not feasible for the criteria related to the MasteryConnect System to be achieved solely by Instructure. Therefore, each user entity's internal controls must be evaluated in conjunction with Instructure's controls, taking into account the types of controls expected to be implemented by the subservice organization as described below.

Complementary Subservice Organization Controls	
1	Access to hosted systems requires users to use a secure method to authenticate.
2	User content is segregated and made viewable only to authorized individuals.
3	Network security mechanisms restrict external access to the production environment.
4	New user accounts are approved by appropriate individuals prior to being provisioned.
5	User accounts are removed when access is no longer needed.
6	User accounts are reviewed on a regular basis by appropriate personnel.
7	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned.
8	Access to physical facilities is restricted to authorized users.
9	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.

Complementary Subservice Organization Controls	
10	Encrypted communication is required for connections to the production system.
11	Access to hosted data is restricted to appropriate users.
12	Hosted data is protected during transmission through encryption and secure protocols.
13	Anti-virus or anti-malware solutions are installed to detect or prevent unauthorized or malicious software.
14	System configurations changes are logged and monitored.
15	Vulnerabilities are identified and tracked to resolution.
16	Security events are monitored and evaluated to determine potential impact per policy.
17	Operations personnel log, monitor and evaluate to incident events identified by monitoring systems.
18	Operations personnel respond, contain and remediate incident events, and update stakeholders, as needed.
19	System changes are documented, tested, and approved prior to migration to production.
20	Access to make system changes is restricted to appropriate personnel.
21	Personnel monitor processing and system capacity on hosted systems.
22	Personnel execute and monitor daily backups. Any identified errors are resolved in a timely manner.
23	Environmental mechanisms provide protection over fire, water, power outages, temperature changes, and natural disasters.
24	Software and recovery infrastructure are implemented over hosted systems.

D. Complementary User Entity Controls

Instructure's MasteryConnect System was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its MasteryConnect System. In these situations, the application of specific controls at these user entities is necessary to achieve certain criteria included in this report.

This section describes additional controls that should be in operation at the user entities to complement the controls at Instructure. User auditors should consider whether the following controls have been placed in operation by the user entity.

Each user entity must evaluate its own internal control structure to determine if the identified user entity controls are in place. User entities are responsible for:

Complementary User Entity Controls	
1	For information requiring explicit consent, the user entity communicates with end users regarding the need for such consent and obtains the consent prior to the collection of information from the data subject.
2	Validating the completeness and accuracy of system outputs.

MOSSADAMS