# Executive Summary

Launched in 2015, MasterClass is the streaming platform where anyone can learn from the world's best. With an annual membership, subscribers get unlimited access to 100+ instructors across a wide range of subjects and new classes all the time. Step into Kelly Wearstler's design studio, Ron Finley's garden and Neil Gaiman's writing retreat. Get inspired by RuPaul, perfect your pitch with Shonda Rhimes, and discover your inner negotiator with Chris Voss. Stream thousands of lessons anywhere, anytime, on mobile, tablets, desktop and Apple TV, Amazon Fire TV® and Roku® devices.

At MasterClass we take the security of our platform seriously. This document will provide an overview of security practices we have in place to help protect the platform and your data. For information regarding privacy, see our privacy policy or our DPA (applicable to our Enterprise License product).

## Information Security Governance

MasterClass maintains a comprehensive set of Information Security Policies which are reviewed and revised at least annually by the security steering committee and approved by management.

## Third Party Assessments

MasterClass validates the effectiveness of its information security program by engaging in a third party assessment utilizing the NIST 800-53 control families. This engagement is performed at least annually by a qualified firm specializing in information security audits and assessments. The results of the assessment are reported to leadership within the organization and are used to continually evaluate priorities associated with remediation and advancements in our control environment.

## Security Steering Committee

MasterClass has a cross-functional security steering committee responsible for security oversight at the company.

## Infrastructure Security

We utilize enterprise cloud providers, including Cloudflare, Heroku, AWS, and GitHub for our platform deployment and operations. These providers are SOC2 and ISO27001 compliant with established security standards and operations.

**More about their security:**

- Heroku Security
- Cloudflare Compliance
- Github Trust and Privacy
- AWS Compliance

## Data In Transit Security

Our website and mobile platforms require Transport Layer Security, or TLS, a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. Masterclass utilizes the most recent version, TLS 1.3, of the protocol for it's public facing web applications.

## _Data At Rest Security

Masterclass utilizes several mechanisms to protect data from unauthorized access while in storage.

- Our data must be encrypted at rest on production databases.
- All employee workstations must have hard disk encryption enabled.
- All media must be stored on encrypted hard drives and tracked through our inventory system.
- Use of personal devices for MasterClass editing and production is not permitted.

## _Operational Security

MasterClass has in place several processes to provide secure access to systems.

- Single Sign On and MFA for corporate applications and production platforms.
- Password Managers are provisioned to every user for safe password and secret storage.
- Security Awareness and Phishing training is provided and required of all employees and contractors.
- Automated provisioning and deprovisioning for business and production applications.

## _Security Engineering

In Engineering, we have several mechanisms in place to protect the security of our code, platforms, and user data.

- Active bug bounty program.
- Enterprise-grade infrastructure and website security tools to mitigate web-based attacks.
- Penetration testing conducted at least annually.
- Static Application Security Testing (SAST) checks in development pipeline.
- Live training to developers regarding application security best practices.
- Robust change management processes.
- Hashing and salting of user passwords.