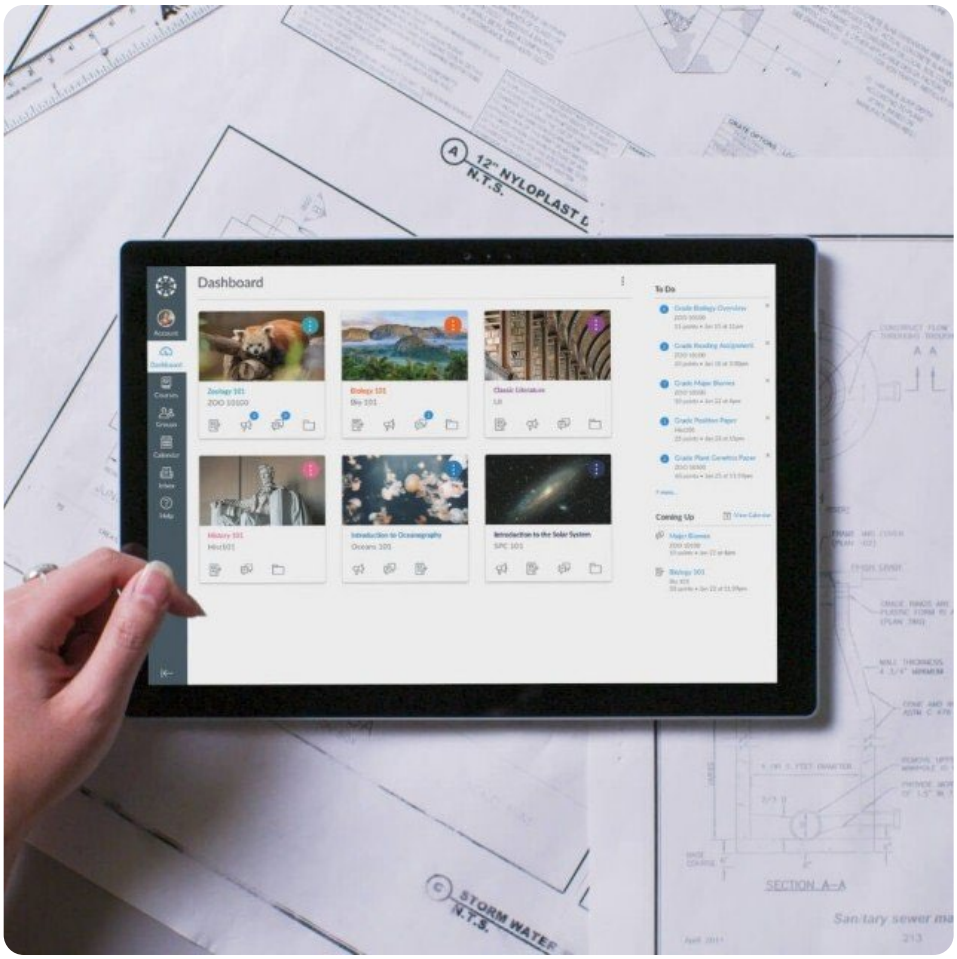
IN THE LOOP. IN THE CLEAR.

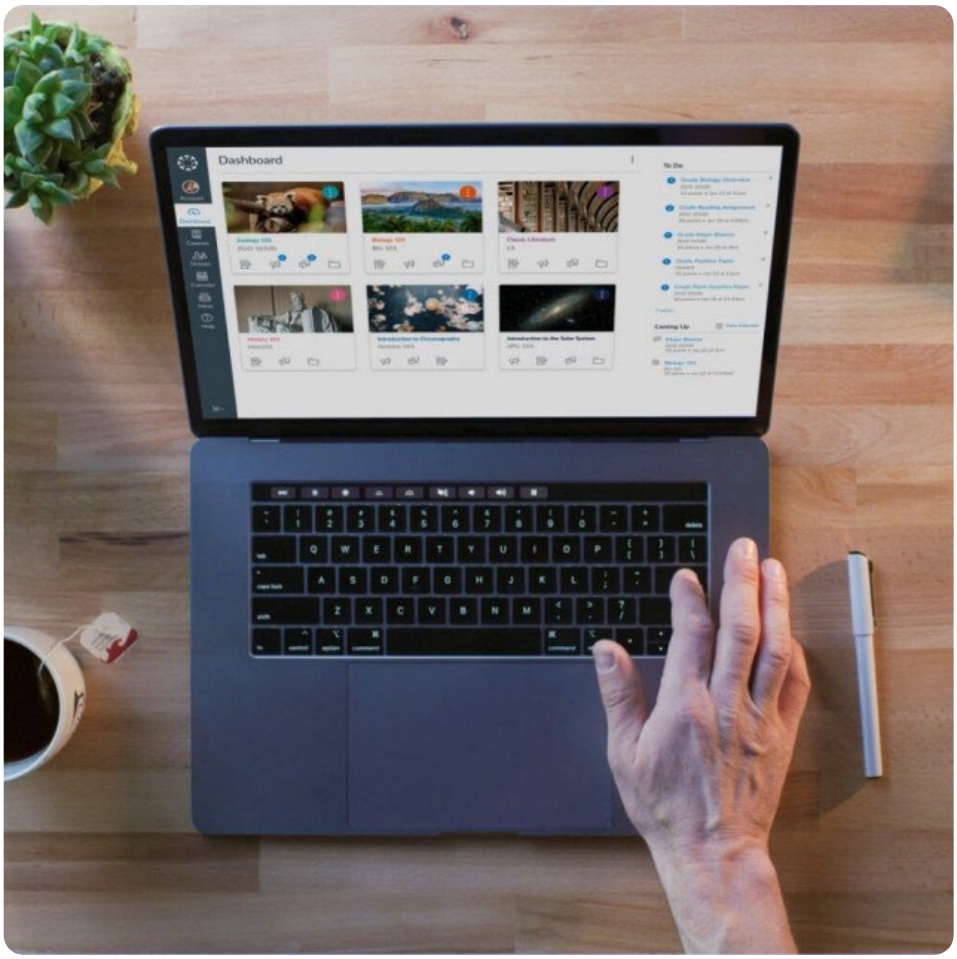
Canvas Has Open Security

That is, we're transparent about the programs and protocols we use to detect bugs and prevent badness.

Security Program and Team

Our security program is built based on ISO 27001, NIST's Cyber Security Framework, AICPA's Trust Services Principles and Criteria, and SANS' CIS Critical Security Controls. And we develop our applications abiding with OWASP's Top 10. 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. We also encrypt data in transit and at rest using known strong cryptographic protocols and ciphers. We produce SOC2 Type 2 reports annually to demonstrate Instructure's compliance with industry best practices for security, availability, confidentiality, processing integrity, and privacy. You can reach out to your customer support manager for a copy of this report. Our dedicated security team is full of passionate, skilled, experienced security professionals who focus on detecting and protecting against badness, and earning and maintaining your trust.


Dashboard
To Do
Coming Up
Zoology 101
Biology 101
Classic Literature
History 101
Introduction to Oceanography
Introduction to the Solar System
SECTION A–A



Security and Due Diligence Documents

Learn more about Instructure's security program and review related due-diligence documents using the links below:

- Instructure Security Whitepaper
- Canvas Architecture Whitepaper
- Instructure Disaster Recovery Whitepaper
- Instructure Business Continuity Whitepaper

Vulnerability Disclosure and Continuous Penetration Testing

Instructure hosts its bug bounty program through Bugcrowd, through which security researchers are continuously poking at our products. We publish—publicly—the results of these activities annually for all to see. You're welcome to join this program and submit your findings. Please send your Bugcrowd ID to security@instructure.com to be added to the program. If you'd like to disclose a vulnerability outside of Bugcrowd, you can send us an encrypted message using our PGP key. (Rewards are paid out through Bugcrowd only.) Download Our Latest Penetration Test Results.

GLOBAL HQ

6330 South 3000 East, Suite 700, Salt Lake City, UT 84121, USA

CONTACT US

800-203-6755

Modern Slavery Act |

Acceptable Use |

Acceptable Use International |

Data Processing

Copyright © 2021 Instructure, Inc. All rights reserved. Various trademarks held by their respective owners.