ellucian

CLOUD SOLUTIONS

Top 10 Security Practices

Data confidentiality, data integrity, and system availability are vital concerns in higher education.

From rigorous external audits to strict security protocols, Ellucian's higher education cloud offerings—which use infrastructure provided by our global cloud provider, Amazon Web Services (AWS)—follow industry best practices to help safeguard the integrity and availability of your most important systems and information.

1. Compliance

Ellucian's higher education cloud offerings in AWS undergo regular third-party compliance audits of our security, availability, and confidentiality controls. These include System and Organization Controls SOC1 and SOC2 reports, which are available to relevant customers and prospective customers (subject to a non-disclosure agreement) in order to support due-diligence efforts. We report on our Cloud Security Alliance (CSA) adherence; model our information security management system after ISO 27001; and align with key components of industry security standards, including the Center for Internet Security (CIS) 20 Critical Security Controls.

2. Data privacy

We're committed to protecting our customers' personal information. We take appropriate measures to treat personal information securely and in accordance with applicable laws and regulations. Ellucian's complete data-privacy policies can be found at www.ellucian.com/privacy.

3. Risk management

As part of our focus on managing and minimizing risk, Ellucian conducts regular internal business-unit risk assessments modeled after the ISO 27001/27002 framework and controls. Third-party vendors are carefully assessed to confirm whether adequate security controls are in place, and third-party relationships are reviewed and classified against risk criteria. Security requirements and contractual provisions are identified and incorporated into agreements as applicable.

4. Security policy

Ellucian's Information Security Policy (ISP) and related standards are modeled after the ISO 27001 framework and communicated to employees and relevant external parties. Ellucian's ISP and standards are reviewed at least once a year—and additionally as needed when a significant change occurs—to provide their continuing suitability, adequacy, and effectiveness.

5. Vulnerability and configuration management

Ellucian is dedicated to maintaining environment integrity in our cloud solutions and defending against unauthorized access and emerging threats. Vulnerabilities identified through our scanning and penetration testing efforts are classified, managed, and remediated according to guidelines. Our rigorous configuration-management program monitors system integrity and security through the use of logging and alerting tools, endpoint antivirus and anti-malware tools, and golden images and configurations.

6. Change management

Ellucian follows defined change-management policies and procedures. These include detailed requirements, reviews, documentation, and classification criteria for changes to systems, software, corporate infrastructure, environments, and data centers. Our process covers both standard and emergency changes and is reviewed annually.

7. Network security and data-protection technology

To protect customer systems and data against hacking and distributed denial of service (DDoS) threats, Ellucian Cloud Solutions uses defense-in-depth with host-based and network firewalls, along with application traffic-monitoring technology. Ellucian Cloud Solutions provides additional protection with Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) protection that is monitored by security analysts.

8. Access control

Ellucian and AWS strictly limit access to information, systems, equipment, and facilities. AWS defines their data centers as tightly secured, where mechanical, electrical, and life-support systems and equipment are constantly monitored to promptly identify issues.

Ellucian follows defined and documented security policies and procedures governing corporate security standards, password parameters, VPN access, and user administration. Access to privileged IT functions is restricted, documented, and tracked.

9. Secure software development

Security is an integral part of the development process and a critical product feature. Our development standards and coding requirements are derived from OWASP practices, and security vulnerabilities are triaged and remediated according to the Common Vulnerability Scoring System and strict internal protocols. We deploy Agile User Security Stories and DevSecOps static and dynamic analysis security testing tools to validate applications, and regularly apply both manual and automated tools to conduct penetration testing and external scans.

10. Incident response

Ellucian's Threat and Incident Response Team (TIRT) is the central reporting point for computer security-adverse events, and may assist operational managers in responding to security events. TIRT's incident response management is based on National Institute of Standards and Technology guidelines, and on the CERT Coordination Center's recommendations. Ellucian's Threat and Incident Management Program supports U.S. Department of Justice-recommended chain-of-custody processes.

"At Ellucian, our customers' data security is paramount."

Namita Dhallan
Senior Vice President and Chief Product Officer, Ellucian

Visit us at www.ellucian.com/cloud

ellucian

Ellucian is the world's leading provider of software and services that power the essential work of colleges and universities.

Visit Ellucian at **www.ellucian.com**.