ellucian

CLOUD SOLUTIONS

Security in Ellucian's Cloud

Key security practices and internal controls that help Ellucian keep your institutional data safe

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

Namita Dhallan
Senior Vice President and Chief Product Officer, Ellucian

Abstract

Campus information systems often house vast amounts of sensitive data. Should a data breach occur, the consequences for exposed individuals can be grave—and the financial and reputational damage to institutions can be severe.

The EDUCAUSE *Higher Education Information Security Council (HEISC)* is driving colleges and universities towards developing "top-notch information security governance, compliance, data protection, and privacy programs." In alignment with that initiative, Ellucian has developed a multi-layered, comprehensive approach aligned with the standards of trusted security frameworks.

This white paper reviews Ellucian's current practices and industry standards for securing cloud-based systems and data—from rigorous independent compliance audits, penetration testing, and security reviews to logical and environmental security. The paper also reviews security practices and internal controls practiced by Ellucian for its Cloud Solutions offerings that use the Amazon Web Services (AWS) cloud infrastructure, making Ellucian the world's leading provider of software and services that power the essential work of colleges and universities.

1 • Introduction

This document contains in-depth security information pertaining to the internal controls at Ellucian and the services that we provide to our customers. The following information can help assess security considerations and questions about Ellucian's Cloud Solutions. The information in this document is considered CONFIDENTIAL and must not be transmitted or disclosed to any third party without permission from Ellucian.

In an ever-changing landscape of technology and security threats, Ellucian will always maintain the right to revise the controls outlined in this document. Ellucian will make reasonable efforts to update this information as improvements are made.

2 • Compliance

SSAE16/18 – SOC 1 and SOC 2 Type II Reporting

The Statement on Standards for Attestation Engagements No. 18 (SSAE18) is the auditing standard for service organizations developed by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). This audit is an independent document that customers and auditors can use to assess financial reports and audits.

Ellucian has retained Ernst & Young LLP to conduct its annual Service Organization Control (SOC) audits. The SOC1 Type II report lists controls implemented at Ellucian and addresses frequently asked questions about Ellucian security processes and internal infrastructure. Ernst & Young also issues a SOC 2 Type II report that is audited against the AICPA standard, with a focus on the Trust Service Principles of security, availability, and confidentiality. Both reports include the auditor's assessment, a description of controls in place, a review of the effectiveness test of each control, and Ellucian management responses to any findings.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of information security standards developed by the PCI Security Standards Council to protect payment cardholder data.

With the release of v.3.2 of the PCI DSS, Ellucian has engaged with a Qualified Security Assessor (QSA) to seek PCI DSS compliance as a Service Provider.

We encourage our customers to consult their institution's QSA (Qualified Security Assessor) or ISA (Internal Security Assessor) to confirm their current PCI status as it relates to their intended use of Ellucian products.

HIPAA (Health Insurance Portability and Accountability Act of 1996)

Ellucian Cloud Solutions in AWS do not currently support the storage of protected Personal Health Information (PHI) that is regulated by HIPAA in our Cloud Solutions products or environments.

Cloud Security Alliance Compliance

The Cloud Security Alliance (CSA) promotes the use of best practices for providing security assurance within cloud computing and provides education about the use of cloud computing best practices to help secure other forms of computing. Ellucian has documented where its Cloud Solutions align with CSA operationally.

In 2017 Ellucian published its self-assessment and alignment with the CSA Consensus Assessments Initiative Questionnaire (CAIQ). This Level One CSA STAR Self-Assessment is published in the CSA registry and is available for customer review at **cloudsecurityalliance.org/registry/ellucian/**.

Internal Audit

A part of Ellucian's information security management system (ISMS) strategy is utilizing Ellucian's internal audit team as an independent group that reports to the audit committee of Ellucian's board of directors. In addition to performing regular internal audits of financial, operational, and technology controls, the team selectively validates and tests Ellucian's internal controls over security practices, processes, and policies.

The internal audit team routinely performs follow-up procedures to validate that remediation activities have been satisfactorily completed. Audit reports are for Ellucian internal use only, but are distributed to executive management, the board of director's audit committee, and applicable business units for remediation purposes. The internal audit group also performs internal audits of Ellucian security controls. Independent third-party validation of the Ellucian information security program is performed during the SOC1 and SOC2 audit efforts.

ISO/IEC 27001:2013 (ISO 27001)

Ellucian's information security program is modeled on the ISO 27001 ISMS framework. ISO/IEC 27001:2013 (ISO 27001) is the international standard that defines best practices for implementing an information security program.

These best practices are a system of processes, documents, technology, and people that helps to manage, monitor, audit, and improve an organization's information security posture.

Reporting Availability

Ellucian's security team provides customers with copies of our most recent SOC1 and SOC2 reports (subject to a non-disclosure agreement), relevant policies and standards, and completed assurance questionnaires demonstrating where we conform with industry security standards, such as the Cloud Security Alliance CAIQ.

Ellucian does not share internal audit or internal risk assessment reports, as these are designed to be internal-facing only. Validation that these audits and assessments occur is captured in the SOC reports.

3 • Data Privacy

Ellucian's privacy policies can be found at **www.ellucian.com/privacy**.

4 • Information Security Management

Ellucian's ISO 27001-based ISMS is intended to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

The ISMS is designed to establish a management framework to initiate and control the implementation and operation of information security within the organization. Ellucian's leadership team actively supports information security within Ellucian through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of its information-security responsibilities.

Ellucian's leadership team has explicitly assigned lead responsibility for information security to Ellucian's chief information security officer (CISO). The CISO has reviewed and approved the ISMS, which demonstrates the commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ISMS. The CISO works with Ellucian's legal advisors regarding compliance with laws and regulations applicable to Ellucian.

5 • Risk Management

Internal Risk Assessment

As part of Ellucian's commitment to minimizing and managing risk, Ellucian conducts internal risk assessments against Ellucian business units to identify unknown risks. These assessments are modeled after the ISO 27001/27002 framework and controls.

Each identified risk is assigned a "security champion" to build a remediation plan as well as any short-term mitigation actions needed to reduce the overall risk to the organization. The status of these risks is documented and reported to senior management regularly.

Ellucian's formal risk acceptance process requires a senior vice president to sign off on a risk that cannot be or will not be remediated in a timely manner. These acceptances are temporary until the risk is addressed.

Third-Party Risk Assessment

Third-party vendors who are identified as affecting the security of our service delivery are assessed according to the Ellucian Third-Party Security Standard. Based on criteria outlined in this standard, vendors are classified into one of three security risk levels. Each vendor is assessed based on these risk levels. Higher-risk third parties have formal risk assessments performed to verify that adequate security controls are in place.

Signed agreements with third parties involved in accessing, processing, or managing Ellucian or customer data document our security expectations with respect to the service delivery they are contractually obligated to.

Third-party relationships are reviewed and classified by Ellucian's security, business owner, procurement, and/or legal teams as appropriate against risk criteria so that relevant information concerning security requirements and contractual provisions are identified and incorporated into agreements and service delivery monitoring processes. Ellucian employees are trained and encouraged to report security incidents.

6 • Security Policy

Ellucian maintains an Information Security Policy (ISP) and related standards that are modeled after the ISO 27001 framework and are defined, approved by management, published, and communicated to employees and relevant external parties.

Ellucian's ISP and standards are reviewed at least annually, and as needed when a significant change occurs, to confirm their continuing suitability, adequacy, and effectiveness. Supporting standards, guidelines, and procedures are adjusted as appropriate.

Organization of Information Security Policy

The ISP and standards cover the following security domains:

- Information Security Management
- Personnel Security
- Asset Management
- Access Control
- Physical and Environmental Security
- Operations Security
- Communications Security
- Systems Development and Maintenance
- Cryptography
- Third-Party Security
- Security Incident Management
- Business Continuity
- Compliance

7 • Information Asset Management

Through the use of enterprise and platform tools, Ellucian keeps records of systems, devices, and data that make up the backbone of the Cloud Solutions offerings. These tools provide a real-time look at what is running in an environment. More importantly, it provides the details necessary to regularly evaluate and review secure deployment practices while maintaining performance.

Asset management also helps provide a baseline for risk and vulnerability assessment, allowing Ellucian to identify and mitigate risks to those assets. These risks are then reported to senior management to build awareness, assess the business risk, and assign resources and priorities to remediate or mitigate that risk for the business and operations.

8 • Information Classification

Information classification allows an organization to implement appropriate security controls and protection criteria to safeguard information based on type. Ellucian's Information Classification Standard defines the classification, labeling, and handling requirements of Ellucian information. The standard applies to Ellucian information assets in the possession of, or span of control of, Ellucian employees, consultants, contractors or temporary staff, business partners, and third parties.

Ellucian classifies data into three primary categories—restricted, confidential, and public—and defines how each category is handled as necessary.

9 • Human Resources

Background Checks

Background verification checks on candidates for employment at Ellucian are conducted in accordance with relevant laws and regulations. These background verification checks may include Social Security number, national identification number, employment history verification, criminal record, and educational background verification.

Employee Security Responsibilities

Ellucian is committed to the training and development of its employees. Employees receive awareness training in, and regular updates about, organizational policies and procedures. Ellucian employees are trained regularly on security awareness and data protection requirements. Employees are required to acknowledge their understanding of and adherence to Ellucian's information security and data privacy policies on an annual basis.

43% of data breaches utilized phishing

Verizon Data Breach Investigations Report (2017)

Employee Data Protection

Employees and contractors have duties and responsibilities to protect information at Ellucian, which are enforced through various policies and procedures within the organization. The duty to observe applicable policies and procedures is a condition of employment. This obligation is also incorporated into Ellucian's Code of Conduct and Privacy Policy. Personal information is treated as restricted information according to our Information Classification Standard and is protected with the highest security measures at Ellucian.

10 • Physical and Environmental Security

Amazon Web Services (AWS) Facilities

Ellucian, an AWS Education Competency Partner, uses AWS for a global, scalable, highly secure, and innovative platform to host many of its Cloud Solutions to better serve higher education customers worldwide. Ellucian chose AWS as its global cloud provider to deliver scale, security, and a rapid pace of innovation. Security and scalability were key elements Ellucian evaluated when choosing AWS.

AWS describes through publicly available documentation that its data centers are housed within nondescript facilities. Mechanical, electrical, and life support systems and equipment are continually monitored to identify issues. AWS performs preventative maintenance on equipment to provide for continued operability. Physical access is controlled by a professional security staff using video surveillance, intrusion detection systems, and other electronic means. Visitors and

contractors are required to present identification sign-in and must be escorted by authorized staff. Two-factor authentication must be provided at least twice in order to access the data center floors.

AWS data center access and information are granted only to contractors and employees with a legitimate business need. Access is revoked upon the conclusion of that business need. Physical access to AWS data centers by AWS employees is logged and routinely audited.

AWS personnel and systems monitor and control temperature and humidity to maintain optimal atmospheric conditions. AWS data centers utilize automatic fire detection and suppression equipment. Smoke detection sensors are located in data center environments, generator equipment rooms, mechanical and electrical infrastructure spaces, and chiller rooms. Areas are protected by wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems. Electrical power systems are designed to be fully redundant. Uninterruptible power supply (UPS) and generators are used to provide backup power in the event of a failure.

Physical and environmental control objectives are validated by AWS's Service Organization Controls 1 (SOC 1), and Service Organization Controls 2 (SOC 2) reports. Ellucian does not provide these reports but can assist customers seeking copies from AWS.

Additional information can be found at **aws.amazon.com/compliance/data-center/controls**.

Ellucian Corporate Facilities

Ellucian implements physical and environmental security controls to protect system resources, the facilities housing those resources, and the facilities used to support their operation. Physical facilities comply with local building codes for structural stability and safety.

Visitors must sign in and obtain a visitor's badge before being granted admittance to Ellucian facilities. Visitors must be escorted. Employees, contractors, and visitors working or visiting the Ellucian facilities must have an Ellucian ID badge or visitor's badge when at Ellucian offices.

Ellucian corporate data centers are operational 24/7/365 and are monitored by CCTV/DVR coverage. Only authorized personnel are permitted access to Ellucian corporate data centers. Access is reviewed to confirm that only individuals with a business need are granted access. Electrical systems are designed to be fully redundant. In the event of a failure, uninterruptible power supply (UPS) and generators are used to provide backup power. Data centers have automatic fire detection and suppression equipment. Temperature and humidity controls are in place to maintain optimal conditions within the data center.

Physical and environmental control systems and equipment are monitored to identify issues. Routine maintenance and testing is performed to keep these systems remain in working order.

11 • Vulnerability and Configuration Management

Ellucian maintains a comprehensive vulnerability management program. Ellucian deploys enterprise-class vulnerability scanning tools to identify risks to its information assets.

In addition, Ellucian partners with a third-party vendor annually to perform penetration testing to assess the security of our Cloud Solutions environments and applications.

Vulnerability Management

Information assets are managed to minimize exposure to technical vulnerabilities in accordance with industry-standard vulnerability management practices. Vulnerabilities identified through vulnerability scanning and penetration testing are classified, remediated, and managed according to the following guidelines for High Risk systems and devices:

Vulnerability Criticality Ranking	Planning Timeframe	Resolution Timeframe
Critical (CVSS 10.0 – 9.0)	3 calendar days	10 calendar days
High (CVSS 8.9 – 7.0)	10 business days	30 business days
Medium (CVSS 6.9 – 4.0)	30 business days	60 business days
Low (CVSS 3.9 – 0.0)	60 business days	90 business days

Any deviations from these guidelines are tracked and monitored internally until remediated.

Configuration Management

Ellucian has defined a strict configuration management program for its Cloud Solutions to provide the integrity and security of the systems that make up the customer offerings.

Through the use of logging and alerting tools, endpoint antivirus and anti-malware tools, and golden images and configurations based on secure configuration best practices, Ellucian works to help maintain environmental integrity and defend against unauthorized access. These images are reviewed regularly to align with newly emerging threats and best practices.

Changes to the golden image are reviewed and approved through a documented change management process.

12 • Change Management

Ellucian has documented change management policies and procedures in place, including requirements for making system and software changes (e.g., network device changes, server upgrades, emergency reboots, ERP bug fixes, etc.). The change management process covers both standard and emergency changes. The policy is reviewed by management on an annual basis.

Each system and application change is documented within a change record maintained in the corporate ticketing system. Each change is assigned a change type based on the estimated risk and effect on the production environment, in accordance with the change management policy and procedures.

Ellucian requires customer approval for changes to the customer's production environment, except those utilizing the Cloud Solutions SaaS model. However, Ellucian does reserve the right to perform emergency maintenance without any prior notification, should it be deemed necessary to protect and maintain the security and integrity of the Cloud Solutions. Confirmation of the customer's change approval is documented in the ticketing system. Changes are reviewed by an Ellucian manager who is a member of the Change Advisory Board (CAB). Members of the CAB are responsible for reviewing, approving, or denying changes.

Changes to the corporate infrastructure, environments, or data centers that support Ellucian Cloud Solutions are managed through a similar documented change management process, with changes documented in the corporate ticketing system.

13 • Network Security and Data Protection Technology

Firewalls

Ellucian Cloud Solutions practice defense-in-depth with host-based and network firewall technology to protect customer systems and data. In addition, Ellucian's application layer protection technology provides protection against well-known and advanced hacking techniques such as SQL injection, cross-site scripting, sensitive data exposure, unvalidated redirects, and many other top web application threats.

Network Traffic Protection

Ellucian Cloud Solutions use network traffic monitoring and protection technologies to protect against malicious activity against customer systems and data. Ellucian Cloud Solutions are monitored 24/7/365 by Ellucian security analysts.

DDoS Protection

This defense-in-depth strategy also provides specific protections against distributed denial of service (DDoS) threats. Ellucian's AWS-hosted Cloud Solutions environments are protected by AWS Shield Standard, a managed Distributed Denial of Service (DDoS) protection service.

More information can be found at
aws.amazon.com/shield/

14 • Access Control

Physical Access

Access to Ellucian's AWS-hosted Cloud Solutions environments is strictly controlled by Amazon. Physical access to AWS data centers is strictly managed both at the perimeter and at ingress points, utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access to their employees and contractors who have a legitimate business need for such privileges. Neither Ellucian personnel nor its customers will have access to AWS data centers.

81% of hacking-related breaches leverage stolen passwords and/or weak or guessable passwords.

Verizon Data Breach Investigations Report (2017)

Application and Environment Access (Customer Role)

Ellucian customers play an essential role in managing access to the Cloud Solutions applications and environments. This flexibility is an integral part of the customer experience when utilizing these services.

Customers maintain responsibility for the day-to-day user administration of the hosted software applications. They manage the designation of users' rights and privileges, determination of password policies, access to specific modules installed, and the timely removal of expired accounts.

As part of their access management, customers are also responsible for the periodic review and timely notification of any needed access changes.

Application and Environment Access (Ellucian's Role)

Ellucian has defined and documented security policies and procedures governing corporate security standards, password parameters, VPN access, and user administration. The policy is reviewed annually by management.

Privileged access to the Cloud Solutions environments at the network, infrastructure, and application layers has been restricted to appropriate Ellucian employees. Access requests are documented and tracked. Processes are in place for the prompt removal of user access upon termination.

Each month, Ellucian management performs a review of users with privileged access at the network and infrastructure layers. The results of the review are documented. Changes to access are documented via Ellucian's corporate ticketing solution.

For customer account access to supporting infrastructure systems, a formal request process is in place to create and remove access. Such requests are documented and tracked to completion. Additionally, Ellucian management performs a review of inactive logins to help customers identify accounts that may no longer be needed.

Remote access to any customer Cloud Solutions AWS environment by authorized Ellucian staff requires the use of VPN and multi-factor authentication.

15 • Secure Environment Design Principles

Segregated Customer Environments

Ellucian uses secure architecture and advanced secure multi-tenancy technology on customer environments.

Ellucian AWS SaaS offerings are protected utilizing multi-tenant secure design principles, while our Application Hosting Services (AHS) customers are protected inside dedicated Amazon Virtual Private Cloud environments to control network traffic and prevent unauthorized access.

Customer Authentication Protection

Ellucian Cloud Solutions provide customers with several secure authentication options, including multi-factor authentication.

16 • Encryption

Ellucian maintains a strong encryption standard, aligned with industry standards, that governs use of encryption technology in Ellucian Cloud Solutions offerings and across the company. These encryption methods are regularly evaluated to address and remediate changes to their effectiveness or security.

Advanced application data encryption is also available to Ellucian customers, allowing for the encryption of sensitive application data completely transparent to the application. Available encryption methods are application-dependent.

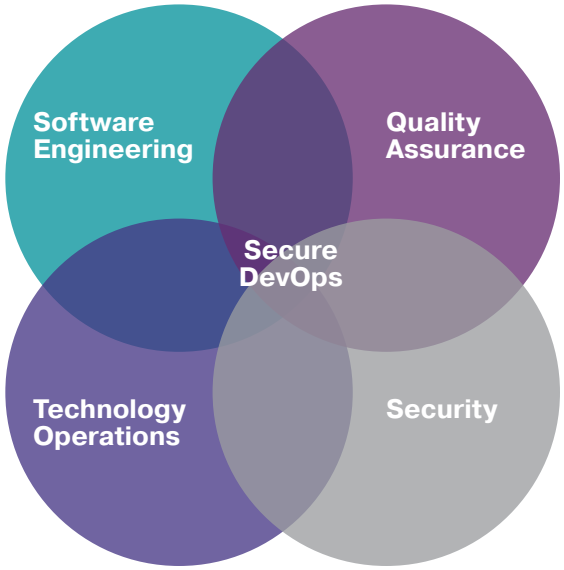
17 • Secure Software Development

Ellucian's Product Security Program is committed to the continuous delivery of application features that contain embedded security. Ellucian uses a comprehensive approach to application development through our Secure Software Development Lifecycle (SSDLC) to make security an integral part of the development process.

Ellucian's Secure Software Development Standard and Secure Coding Requirements are derived from OWASP practices such as the Application Security Verification Standard (ASVS). Developers receive annual secure coding training, supporting these requirements.

Security vulnerabilities are triaged and remediated according to the Common Vulnerability Scoring System (CVSS), Ellucian's Vulnerability Management Standard, and our Product Defect pipeline. Additionally, Ellucian has integrated secure development practices, such as secure software design, coding and testing, and best practices for processing and handling sensitive data.

The SSDLC is the foundation of Ellucian's Product Security initiative, which includes static and dynamic analysis security testing to validate applications. In addition to automated tools built into the DevOps pipeline, Ellucian also undergoes third-party manual penetration testing and external scans on a recurring basis to identify additional potential vulnerabilities.



18 • Business Continuity and Disaster Recovery

The Ellucian Disaster Recovery Plan (EDRP) is a living document maintained and updated regularly by various teams within Ellucian. It includes critical disaster recovery (DR) planning assumptions and establishes the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The EDRP directs business units within Ellucian on procedures for rapid restoration of critical functions within our Cloud Solutions environments.

Our EDR plan consists of four phases:

Phase 1: Disaster assessment and notification procedures
Phase 2: Incident and disaster recovery team activation
Phase 3: Restore critical operations / Customer environment / Regular communication
Phase 4: Root cause analysis and mediation plan for the failure

Our hosting partners deploy and maintain a minimum of N+1 redundancy throughout the physical infrastructures where Ellucian Cloud Solutions are hosted:

- Networks, storage, servers, generators, power plants, etc.
- Elastic IP addresses for consistent and re-mappable routes
- Multiple regions and EC2 Availability Zones (AZs)
- Real-time monitoring via Amazon CloudWatch, Solarwinds, and/or Logic Monitor
- Amazon Elastic Block Storage (EBS) is highly redundant across multiple regions and Availability Zones
- Elastic Load Balancing on multiple layers for separation of Web Frontends, Applications, and Databases

19 • Incident Response

Threat and Incident Management Program

Ellucian's Threat and Incident Management Program supports U.S. Department of Justice-recommended chain-of-custody processes including forensic data collection, preservation, and analysis.

Threat and Incident Response Team

Ellucian's Threat and Incident Response Team (TIRT) is the central reporting point for computer security adverse events, incidents involving personal data, and incidents affecting the Ellucian network infrastructure if determined malicious in nature.

The TIRT will assist Ellucian's legal and human resources departments, as well as the Security Risk and Compliance, Research and Development, and other relevant teams, in taking the appropriate actions necessary to contain, mitigate, and resolve information security incidents. The TIRT may assist operational managers in responding to security events.

Threat and Incident Framework

The TIRT Team follows the National Institute of Standards and Technology's recommended Incident Response Life Cycle (Computer Security Incident Handling Guide, NIST SP 800-61):

- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident activity

The TIRT code of conduct is based on the CERT Coordination Center's recommendations. The incident type, cause, and/or severity will dictate the action required for resolution.

Threat and Incident Handling

Ellucian employees and customers are directed to contact Ellucian Global Information Security via the Central Help Desk. The Central Help Desk dispatches accordingly to the TIRT.

20 • Summary

As the leading global provider of higher education software and services, Ellucian offers a complete set of integrated cloud-based applications and services that help colleges and universities improve performance and solve key institutional challenges—from recruiting and student success to continuing education and advancement. Our Cloud Solutions are built specifically for higher education and developed to maximize the power of the cloud.

Ellucian delivers one-stop access to top-tier data center environments, high-speed Internet connectivity, technical expertise, monitoring, security, backup, and disaster-recovery services. As a leader in SaaS and application hosting security, Ellucian has built many of its Cloud Solutions on the reliable and secure backbone of Amazon Web Services' Infrastructure as a Service (IaaS).

Ellucian aligns itself with industry best practices and complies with key standards and regulations. Ellucian's information security program is modeled on the ISO 27001 ISMS framework, and we utilize the Cloud Security Alliance's guidance for cloud platform initiatives. Each year, Ellucian retains Ernst & Young LLP to conduct its annual Service Organization Control (SOC) audits. The SOC1 and SOC2 Type II reports are available to customer for review upon request and execution of a non-disclosure agreement.

In addition to cloud software application options purpose-built for higher education, Ellucian offers cloud application hosting services and the infrastructure and technical expertise customers need to manage their Ellucian applications. Ellucian also offers expert services to manage customers' infrastructure and enterprise systems, freeing customers to focus on more strategic priorities.

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.**