**COMPLIANCE**

**Frameworks**

Parchment information security management system is based on industry best practices ISO 27001, NIST CSF, PCI DSS. Through these frameworks, members and learners can trust that working with Parchment is a reliable, consistent, and secure experience.

**ISO**

* ISO 27001:2013 (ISO 27001) is an international standard that helps organizations manage the security of their information assets. It provides a management framework for implementing an ISMS (information security management system) to ensure the confidentiality, integrity, and availability of all corporate data (such as financial information, intellectual property, employee details or information managed by third parties).

The ISO 27001 framework was published in 2013 by the ISO (International Organization for Standardization) and belongs to the ISO 27000 family of standards. It is the only internationally recognized certifiable information security standard. ISO 27001 is supported by its code of practice for information security management, which explains how to implement information security controls for managing information security risks.

These certifications run for 3 years (renewal audits) and have annual touch point audits (surveillance audits).

*The Information Security Management system is designed to support a mission of Turning Credentials into Opportunities through the delivery and support of learner Accounts. Parchment Award, Parchment Pathways, Parchment Services, and Parchment Digitary (CORE, MyEquals, and MyCreds) across the K12, Higher Education, International and Workforce markets.*

*Including the technologies, staff, policies, and office locations in accordance with the State of Applicability v2023. 1*

**SOC2 Type II**

* Annually, Parchment undergoes SOC2 Type II audit by a third-party [AICPA](https://us.aicpa.org/content/aicpa) firm to ensure customers are protected across various levels. The scope of the SOC2  Type II audit covers all of [Parchment Products](https://www.parchment.com/products/) and emcompnases all five Trust Servce Criteria, inducing Security, Confidentiality, Availability, Processing Integrity, and Privacy.

**PCI**

* The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS is a set of network security and business best practices guidelines adopted by the PCI Security Standards Council to establish a “minimum security standard” to protect customers’ payment card information. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.
* Parchment maintains compliance with PCI DSS, as a level one Service provider. To ensure credit card data is securely handled Parchment has Partnered with Chase to provide a secure and reliable payment process. Parchment does not directly store, process, or transmit any cardholder data. Parchment undergoes annual Report on Compliance assessment by Qualified Security Assessors against the current PCI DSS requirements. We can provide a copy of our Attestation of Compliance upon request.

**FERPA**

* The Family Educational Rights and Privacy Act (FERPA) is a federal law enacted in 1974 that protects the privacy of student education records. Parchment handles all requests and access to FERPA protected records in a secure and compliant manner, always requiring consent as needed and preventing unauthorized disclosure.

**Accessibility VPAT 508 Compliance**

* Parchment is [committed to making its services accessible](https://parchmentsupport.force.com/s/article/Accessibility-to-Parchment?language=en_US) to individuals with disabilities by meeting or exceeding accessibility standards. We target compliance with the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA guidelines in the design and development of Parchment services. Conformance with these guidelines makes Parchment more accessible and user friendly for everyone. We enhance and test Parchment services regularly to maintain compliance with this standard.
* A Voluntary Product Accessibility Template is a document used by providers to self-disclose the accessibility of a particular product. We are happy to provide a copy of the product specific VPAT upon request.

**PRIVACY**

We are deeply committed to learner and member privacy and embrace privacy by design in everything we do. Transparency builds trust, and we strongly believe in informing all of our users about their [**Privacy Rights**](https://www.parchment.com/privacy-policy/) and [**Terms of Use**](https://www.parchment.com/terms-of-use/). If you have any questions or concerns regarding Privacy, please contact [**Privacy@parchment.com**](mailto:Privacy@parchment.com)

**GDPR and CCPA**

Parchment handles personal information with compliance in mind. Our platform is General Data Protection Regulation (GDPR) compliant and meets the California Consumer Privacy Act (CCPA) standards. Please reference Parchment’s [**Privacy Policy**](https://www.parchment.com/privacy-policy/), [**Data Protection Addendum**](https://www.parchment.com/data-protection-addendum-2021/), and designated [**Suprocessors**](https://www.parchment.com/subprocessors/). If you wish to exercise any Privacy rights, please contact us at [**Privacy@parchment.com**](mailto:Privacy@parchment.com)

**SECURITY CONTROLS**

**Availability & Reliancy**

Parchment systems are hosted on Amazon Web Services ([**SOC 1, SOC 2, and SOC 3 certified**](https://aws.amazon.com/compliance/soc-faqs/)) deployed across multiple availability zones. Providing our members and learner communities with trusted [**Uptime and Reliability**](http://www.status.parchment.com/).

**Vulnerability Management**

A formal Vulnerability Management Program to proactively identify and remediate technical vulnerabilities in its systems, applications and services. Please contact us through our [**Responsible Disclosure page**](https://www.parchment.com/responsible-disclosure/) to report any suspected vulnerabilities.

**Network & Transmission Protection**

Parchment implements appropriate technical solutions to protect the confidentiality and integrity of network communications. Baselines of network traffic and expected data flows to identify what activities that would be considered anomalous behavior. Parchment leverages AWS Security tooling that includes; GuardDuty, CloudTrail, Security Hub, & Inspector, as well as an enterprise SIEM.

**Audit, Logging, & Monitoring**

Parchment leverages the AWS Well-Architected framework to build secure, high-performing, resilient, and efficient infrastructure for all Parchment Products.

To ensure the effectiveness of our security measure, and detect potential security events, auditing, logging and monitoring are enabled throughout our AWS environment, and the application.

**Software Development**

Security is considered in the entire end-to-end process of developing software, including [**OWASP**](https://owasp.org/) training, processes, code reviews, and vulnerability scanning.

**Risk Management & Incident Response**

Risk management is continuously in place for both internal and external sources.  We take a proactive approach to performing risk assessment. Potential security risks or events are evaluated and reviewed continuously. Formal incident response plans are in place and tested.

**Data Protection**

Data integrity and confidentiality are obtained through extensive encryption of data, both in transit and at rest, and role based access controls.

**SECURITY ASSESSMENTS**

Parchment understands the importance of vendor management and due diligence. Our Information Security team wants to assist you in providing a timely response to your security questions and assessments. Parchment has a streamlined process to complete your requests when considering partnering with us. If your Vendor Risk Management process is based on the [**EDUCAUSE**](https://www.educause.edu/)HECVAT, we can share our pre-completed questionnaires. If your Vendor Risk Management process is based on 3rd party auditor attestations or reports, Parchment is happy to provide copies of our PCI Attestation of Compliance and/or SOC2 Type II report. Parchment’s ISO 27001 certification is also available by request. Please contact your Regional Sales Representatives or Account Executive to get the process started, or submit us a ticket in our [**Help Center**](http://support.parchment.com/).