lumen

Lumen Learning LLC Security and Operations Policy

Updated August 11, 2017

Lumen | 600 NW 14th Avenue, Suite 200 | Portland, OR 97209 | 971.303.9637 | www.lumenlearning.com

lumen

Contents

Introduction

Information is a key resource for Lumen, without which virtually all of our activities would cease. Our information includes: SaaS service offerings, administrative, personnel, financial and funding data; computing network and database systems, methodology; analyses; publications and references. Information may exist in many forms: it may be printed or written on paper, stored electronically, transmitted using electronic means, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Lumen will protect its information assets in ways that are both appropriate and effective. This will help enable Lumen to fulfill its responsibilities and to enable our staff to continue their mission and to provide service to our clients.

Our ability to protect our information assets will enable us to maintain and improve our reputation and ensure that we meet our business and professional goals. In addition it will ensure that we do not lose opportunities for partnership or our ability to service our clients.

lumen

Objective

Our objective is to protect Lumen's customers, users, operations and professional standing from security issues.

Security issues can include confidentiality (people obtaining or disclosing information inappropriately), integrity (information being altered or erroneously validated, whether deliberate or accidental) and availability (information not being available when it is required). A wide definition of security will be used to include all types of incident that pose a threat to the effective use of information. This includes performance, consistency, reliability, accuracy and timeliness.

Principles

We will:

- Use all reasonable, appropriate, practical and effective security measures to protect our clients' important processes and assets in order to achieve our security objective.
- Continually review our use of security measures so that we can improve the way in which we protect our business.
- Protect and manage our information assets to enable us to meet our contractual, legislative, privacy and ethical responsibilities.

Roles and Permissions

All staff, past and present, permanent, honorary, and temporary of Lumen have an obligation to protect our information assets, systems, and infrastructure. They will, at all times, act in a responsible, professional, and security-aware way, maintaining an awareness of and conformance to this Policy.

Everyone will respect the information assets of our clients and third parties whether or not such protection is required contractually, legally or ethically.

All members of Lumen are responsible for identifying security shortfalls in our existing security practices and/or improvements that could be made. These should be reported to the Information Security Officer (ISO).

All members who have supervisory responsibility are required to actively promote best practice amongst their supervised staff.

Defined Roles and Permissions

Lumen's security roles and their permissions are as follows:

- Course and Content Developer

    - These staff have access to the content platform for creation and editing of course material. They may have access only to anonymized student data, if any. Lumen often employs contractors at this security level, but they are restricted to specific sets of content.
- Support Staff
    - Support members have access to customer data that is made available through Lumen's application interfaces.
- Software Development Staff
    - Developers often have full data access to the projects they are directly working on. This access is controlled by the Director of Development. This staff also has access to all of the Lumen Platform system code.
- Director of Development
    - The Director of Development has access to all Lumen data and controls access for others. The Director has ultimate responsibility for ensuring that information within Lumen is adequately protected. The Director will delegate responsibility for approving and reviewing access rights to information to named, responsible individuals.
- Executive Committee
    - The Lumen executives do not have direct access to data beyond a Support Staff level, but are in charge of policies and guidance to the Director of Development.
- Researchers
    - Lumen partners with researchers as part of the Learning Lab program. See the Data Privacy section for more details.

When an employee is hired they are given access to their appropriate level. Any access needed beyond the pre-designated scope will go through the Director of Development.
When an employee is terminated, their access is removed immediately.

Hosting Partners

Lumen works with world-class hosting partners. Lumen has 3 primary hosting partners:

- Amazon
    - Lumen hosts data and multiple applications on Amazon's AWS system.
- Pantheon
    - Lumen hosts a Wordpress content system with Pantheon.
- Blackmesh
    - Lumen hosts a Wordpress content system with Blackmesh on virtual private servers.

All physical server security is handled by these partners.

lumen

Data Privacy

Lumen staff uses and manages different types of data which require different levels of security.

Types of Data

The types of data used and managed by Lumen are:

1. **Personal**: Includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.
2. **Public**: Includes openly licensed content and attributions, already-released marketing material, commonly known information, etc. There are no requirements for public information.
3. **Operational**: Includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data falls into this category, including learning data, enrollment data and integration information.
4. **Critical**: Any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.
5. **Confidential**: Any information deemed proprietary to the business. See the Confidential Data Policy for more detailed information about how to handle confidential data.

Data Security

Data security is maintained by the Roles and Permissions used within Lumen and with security best practices on the Lumen Platform. Together with our hosting partners we continually improve on our security best practices. Our hosting partners monitor and patch system-level security problems. Our development staff monitor and patch application-level security problems.

LTI Credentials

Lumen Learning courseware is delivered into institutional customer's Learning Management Systems (LMSs). LTI credentials used to integrate the Lumen platform with customer LMSs are unique to each customer and are shared with customers in a secure fashion.

Learning Data Practices

Lumen Learning adheres to transparent, responsible and ethical practices around data ownership, sharing and use. Lumen Learning is also committed to compliance with institutional, state and federal policies regarding appropriate handling and use of learner data.

Learning data is captured to support the proper functioning of the courseware and learning science research. Lumen Learning seeks to advance learning science by yielding insights about

learning and how to improve learning efficacy using data collected through courseware as well as related learner data from institutions.

Specific data captured by Lumen courseware include:

- De-identified usage information
- Personally identifiable information (PII) including name, email, usage and assessment results to facilitate a variety of personalized functions within the courseware (e.g. personalized feedback and teaching interactions)

Lumen Learning's understanding is that any and all data created by students through their use of Lumen Learning's systems during the course of the engagement are owned by the students. Because they are the creators of these data, US law automatically vests copyright in the students. Use of a system or technology in the creation of data does not interfere with this grant of rights, in the same way that Microsoft does not hold copyright in the documents an individual creates in Word or the presentations a person creates in Powerpoint. Neither Lumen Learning nor their institutional partners can make an ownership claim on data created by students simply because they use our systems to create them.

Where appropriate, we seek consent from students and faculty to use learning data for research and analytical purposes, following best practices established by Carnegie Mellon University's Open Learning Initiative (OLI). Implemented with process oversight from Brigham Young University's Institutional Review Board (IRB) and Carnegie Mellon University's Institutional Review Board (IRB), this approach uses an opt-in/opt-out form to confirm user consent for authorized researchers and research communities to use their de-identified data in research studies. Students may opt in or opt out repeatedly, allowing them to change their minds about participation at any point. Lumen Learning's use of learner data from outside the courseware is governed by agreements with participating institutions that contribute additional learner data to Lumen Learning projects.

For more detail about Lumen Learning's data and research practices, please see our published policy statement on this topic: lumenlearning.com/data-practices

Data Retention

We maintain nightly, weekly, and monthly database backups. Nightly, weekly, and monthly database backups are maintained by hosting partners Amazon and Pantheon according to partners' documented procedures.

lumen

Testing and Reporting

Security Testing

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the company's network security. We perform frequent internal security audits and work with our hosting partners to continually assess security needs and practices. All application code is reviewed for security purposes before it is deployed.

Communication of Incidents

In the event of a breach, the Director of Development will notify the Executive Committee, and the Executive Committee will communicate with affected customers and coordinate a response to the incident.

Security Policy Review

The company's security policies are reviewed at least annually. Additionally, the policies are reviewed when there is an information security incident or a material change to the company's security policies. As part of this evaluation the company reviews:

- Any applicable regulations for changes that affect the company's compliance or the effectiveness of any deployed security controls.
- If the company's deployed security controls are still capable of performing their intended functions.
- If technology or other changes have an effect on the company's security strategy.
- If any changes need to be made to accommodate future IT security needs.