Cloud Computing Security

Security Considerations for Cloud Computing

Security, privacy, identity, and other compliance implications of moving data into the cloud.

1. **Confidentiality and Privacy**
    a. Institutions are obligated by regulations such as HIPAA or FERPA to protect educational records, yet placing those records in the cloud introduces new risk. "*Education records*...means those records that are: (1) Directly related to a student; and (2) Maintained by an educational agency or institution or by a party acting for the agency or institution".
    b. Export controls (such as ITAR).
    c. If some information is FOIA-able what granularity is data defined and managed.
2. **Data Breach Responsibilities and Security**. *Placing data and services in the cloud amplify concerns about data breaches, yet security is not under direct control of the institution.*
    a. Data breach generally carries with it an obligation to notify. Who is responsible for notification (you, vendor, 3rd party) and how quickly.
    b. Risks to intellectual property: authorization, terms and conditions that (inappropriately) assert ownership over IP held by third parties, weakening of ability for institutions to assert "work made for hire" for creations that are developed "without use of institutional resources".
    c. Export controls. Does the vendor house data at foreign sites? Are the systems managed by foreign nationals?
3. **E-Discovery**
    a. Institutions and their legal counsel may be obligated to keep records needed for legal discovery. But these records are not under direct institutional control; the institution no longer has the record in the same way that it formerly did. How does one 'discover' within this externalized infrastructure? (See the E-Discovery Toolkit for more information.)
4. **Risk Evaluation**
    a. Indemnification (both ways)
    b. Warranties (and lack thereof)
    c. Responsibility for End Users
    d. Patent Infringement
    e. Choice of Law and Jurisdiction
    f. Risk Transfer
    g. Procurement Policies & Practices (e.g., procurement policies should require a risk evaluation for products that store records with confidential data)
    h. The University of Florida's Office of Security and Compliance has provided a template that may be used by other institutions to perform a cloud risk survey: SaaS Security Assessment Questionnaire for Hosting Service Provider. There are many additional resources (templates, guidelines, tools) in the Risk Management chapter of this guide.
5. **Business Continuity**
    a. Suspension/Termination and their Aftermath
    b. Service Level Agreements
    c. Fungibility of service (how portable is the data if looking to move to a different cloud provider)
6. **Legal Issues & Third Party Obligations in Cloud Computing Contracts**
    a. Grants with Stipulations
    b. Course Management
    c. Risk Transfer
    d. Consider incorporated website terms that are modifiable at will. Since the terms of some contracts are tied to URL's that are modifiable at will, new risk can be introduced without conscious evaluation of it. How does one evaluate a river? Does one ever step into the same river twice? (Is there a service like the WCA to freeze a URL and tie it to a specific time-set of data)
    e. Legal and Quasi-Legal Issues in Cloud Computing Contracts
    f. Data Protection Contractual Language: Common Themes and Examples

Additional Resources for Cloud Computing Security

Higher Education Resources

- Cornell University: Outsourcing and Cloud Computing for Higher Education
- Indiana University: Use of Cloud Computing
- Rhode Island School of Design: Legal and Quasi-Legal Issues in Cloud Computing Contracts
- Texas State University: Guides for Cloud Computing and Using non-Texas State Information Services
- University of California: Cloud Computing Task Force Report to the Information Technology Leadership Council(Final Report, January 8, 2010) and DRAFT White Papers
- University of Florida: SaaS Security Assessment Questionnaire for Hosting Service Provider (*Note: This is a template that may be used by other institutions to perform a cloud risk survey.*)
- University of Oregon: Cloud Computing Security Slides (by Joe St Sauver)
- University of Wisconsin-Milwaukee: Cloud Computing Resources
- EDUCAUSE's 7 Things You Should Know About Cloud Computing
- EDUCAUSE Cloud Computing Workshop: Suggested Readings on Cloud Computing and Shared Services and Cloud Computing in Higher Education Primer
- EDUCAUSE Resource Pages: Cloud Computing, Cloud Services, E-Discovery, E-mail Management, and Outsourcing
- HEISC Resource: Data Incident Notification Toolkit
- HEISC Resource: Data Protection Contractual Language: Common Themes and Examples
- HEISC Resource: E-Discovery Toolkit
- HEISC Resource: Mobile Internet Device Security Guidelines

Industry & Other Resources

- Burton Group: Cloud Computing--Transforming IT (presentation at the 2009 ECAR Symposium)
- Cloud Security Alliance (CSA)
- CSA's Security Guidance for Critical Areas of Focus in Cloud Computing
- GAO Report: Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing

- GAO Testimony: Information Security: Governmentwide Guidance Needed to Assist Agencies in Implementing Cloud Computing
- Gartner: Know Your Rights in IT Maintenance and Cloud Computing (includes links to several cloud resources)
- Gartner Free Report: Rights and Responsibilities for Consumers of Cloud Computing Services
- Google Apps for Education: Infrastructure Security
- Google Enterprise Blog: Security First: Protecting Your Data With Google Apps
- Google Security Whitepaper: Google Apps Messaging and Collaboration Products
- PCWorld: Lawmakers Question the Security of Cloud Computing
- Pew Report: The Future of Cloud Computing
- Shared Assessments Program
- Shared Assessments Program: Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide
- SANS: Cloud security blog

Questions or comments? Contact us.