



CLOUD COMPUTING GUIDING PRINCIPLES

The rapid growth of cloud computing offers tremendous potential for efficiency, cost savings and innovations to government, businesses and individuals alike. The key features of the cloud are the ability to scale and provide as needed data storage and computing power dynamically in a cost efficient way, without the user having to manage the underlying complexity of the technology.

These benefits will improve government services and citizen access; transform businesses; provide new innovations to consumers; improve important services, such as health care and government-provided services; and create energy savings.

Achieving the full potential of cloud computing requires cooperation between governments, industry, and individual users. To realize this transformative potential, we must:

- ⇒ build confidence in the cloud by protecting users' interests,
- ⇒ promote the developments of standards and needed infrastructure,
- ⇒ clarify laws and policies to promote investment in cloud computing.

We believe the following factors and policies are key to promoting the development and adoption of efficient and innovative cloud computing services:

1. Security

Cloud users need assurance that security risks associated with storing their data and running their applications on cloud systems are understood and appropriately managed. This is as true for government users as it is private users.

To achieve the needed security cloud service providers must adopt comprehensive security practices and procedures including:

- Well-recognized, transparent and verifiable security criteria.
- Robust identity, authentication and access control mechanisms commensurate with the level of sensitivity of the data.
- Comprehensive and ongoing testing of security measures before and after deployment.

2. Combating fraud and other illicit acts

Illicit activities in cloud computing environments such as digital theft, fraud and malicious hacking are a threat to both users of the cloud and service providers.

- Applicable laws should be updated to provide meaningful deterrents and clear criminal and civil causes of action against fraud, malicious hacking and other harmful activity, and new laws should be enacted where needed.

3. Interoperability

Data portability and seamless use of interoperable applications are key consideration for all cloud users.

- Cloud providers must work together to ensure that interoperability and portability are addressed through open collaboration and the appropriate use of standards and by using and adopting existing standards wherever appropriate
- Government agencies should permit standards for interoperability and portability to be developed in industry-led standards processes. The government should convene industry to accelerate standards development and share its user-requirements with industry-led, open standard setting organizations.
- As the government develops and deploys cloud computing solutions it should disclose its requirements to the public.

4. Privacy

Cloud users need assurance that their private information stored, processed and communicated in the cloud will not be used or disclosed by the cloud provider in unexpected ways.

- Cloud providers should establish privacy policies that are appropriate for the particular cloud service they provide and business model they employ. They should make full and prominent disclosure of such policies and should give reasonable advance notification to their customers of any changes in those policies. When appropriate, they should provide customers with the opportunity to opt out of such changes.
- Governments should accord similar protections from disclosure to the government of data held by cloud providers as are currently applied to data held on a person's own computer or within a business' on-premises data center.

5. Protecting intellectual property rights

Providers of cloud computing technologies and services, as with other highly innovative technologies, rely on patents, copyrights and other forms of intellectual property protection.

- Intellectual property laws should provide for clear protection and vigorous enforcement against misappropriation and infringement.

6. International Harmonization of Rules

National governments have implemented, or are developing, sometimes conflicting legal obligations with respect to user data and content held by cloud computing service providers. These conflicting obligations impede innovation and undermine consumer confidence in the cloud.

- Governments, in consultation with industry, should work to harmonize rules in areas such as data protection that affect cloud computing.

7. Promoting free trade

Cloud technologies operate across national boundaries and their success depends on access to global markets.

- Countries should commit to a moratorium on implementing policies that create actual or potential trade barriers to the evolution of cloud computing and should assess existing international trade rules and update them where needed.