

21 Steps *to the* Cloud

These best practices will help you arrive at better service contracts!

The Center for Digital Government's *Guide to Cloud Procurements* includes 21 model contract terms developed by a team of 12 governments and 14 companies – all designed to help public agencies buy software, infrastructure and platforms as a service. The guide, available at govtech.com/procurement, provides nearly 80 pages of pure procurement satisfaction. 21 Steps to the Cloud gives you a taste of what's inside.

Data

Governments have a fundamental responsibility to limit access to non-public data and protect data integrity. These steps cover data ownership and management concerns.

Protect sensitive data by requiring encryption.

Define provider data access narrowly – just enough to deliver the service.

Insist that providers use only U.S. data centers – but let tech support “follow the sun.”

Affirm your right to import and export data whenever you need to.

Identify data roles and responsibilities, but remember that you own the data.

Require providers to notify you of unauthorized data theft or disclosure within 24 hours, or sooner if required by state law.

Cap provider liability for data breaches – use a set amount per record or per person.

Make sure your cloud company tells you about e-discovery or other legal requests.

Agree on a format and timeframe for providers to return your data if a service terminates.

Few providers will agree to unlimited liability for security breaches. If your contract demands it, you'll have trouble attracting bidders.

Make sure cloud companies perform background checks on employees and subcontractors.

Software as a Service
Service provider owns and operates all software and hardware needed to provide the service.

Require your provider to disclose non-proprietary security processes.

Classify your data by security category, then match your cloud provider's security to the data classifications.

Demand access to provider security logs and reports; spell out reporting formats in an SLA.

Providers shouldn't store sensitive data on mobile devices; if data has to be mobile, make sure it's encrypted at rest.

Infrastructure as a Service
Hosted processing, storage and network resources that can be quickly provisioned to run your own applications.

Establish your right to remove contractor staff and spell out the conditions for doing so.

Providers will struggle to estimate their costs if they don't have a clear understanding of the appropriate level of control and security for your data.

Security

You'll need to perform due diligence on your service provider's security practices. These steps will help ensure your data is safe.

Specifying traditional auditing practices in your contract can be a barrier to acquiring services.

Require your cloud provider to perform independent audits of its data centers annually.

Personnel

Public jurisdictions must guard their data no matter where it is. Protect yourself from internal data security threats by following these steps.

Audit your cloud company to ensure it's conforming with the contract.

Audits

Oversight and control are critical for any public expenditure. These steps will help you tailor audits to fit the service model.

Platform as a Service
Hosted infrastructure where you can create or acquire applications using tools and programming languages supported by the service provider.

Make sure you get advance notice of upgrades or system changes.

Require disclosure of all subcontractors and business partners involved with your apps and data.

Insist on a detailed business continuity and disaster recovery plan from your provider.

START

Operations

Use these steps to assure that your cloud provider's system performance and service reliability meet your needs.

WELCOME TO THE CLOUD!

Breach Notification

Prompt notice of a security incident gives agencies time to take appropriate action. Defining provider liability for a data breach can be difficult. These steps can help.