Microsoft

Transforming Governments:

Cloud policy framework for innovation, security, and resilience

Cloud computing represents a seismic shift when compared to traditional computing, enabling governments to do more, faster. **It is advancing governments' ability to communicate directly with their citizens, as well as enabling the implementation of new ideas while unleashing a whole new generation of transformation, delivering big data analytics and empowering the Internet of Things.** In short, governments that successfully implement cloud computing will not only be able to deliver efficient and cost-effective services but also will earn innovation, security, and resiliency dividends.

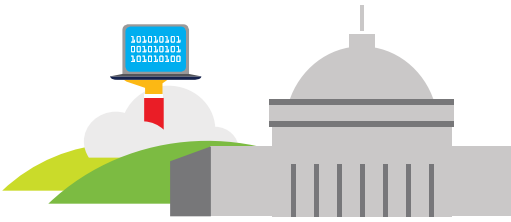
However, understanding how to make the right policy, operational, and procurement decisions can be difficult with any new technology, and doing so can seem especially daunting with cloud computing because it has the potential to alter the paradigm of how business is done. More specifically, confusion about appropriate legislative frameworks and specific security requirements of different data assets risks slowing government adoption.

Microsoft has long supported the notion that governments should develop a national strategy for cybersecurity to guide their effective management of challenges and opportunities in an era of information and communication technologies (ICT). In addition, to support government transitions to cloud technology and advance government innovation, security, and resiliency, Microsoft offers six cloud security policy principles to guide the next generation of ICT policy. Security and resilience have been identified as prime areas of focus because they have become essential to successful operation of modern governments' ICT systems. Importantly, governments must not wait for a crisis situation to establish their cloud computing strategies and to test their plans for achieving ICT resilience and security. Rather, whether they use public cloud services by default or as a failover option in crises for more sensitive data, governments must be confident that, if a crisis does unfold, the integrity and availability of their data and essential services will remain intact.

The principles are intended to guide governments as they balance the benefits and risks of migrating to cloud platforms and solutions. In particular, they focus on how to use cloud computing to achieve security and resiliency of government operations, a critical foundation of any technology implementation. They are grounded in what we believe to be best practices pursued by various governments that have already tested and trusted the cloud. They also build on the commitments that Microsoft puts at the heart of our trusted cloud: security of operations, data protection and privacy, compliance with local requirements, and transparency in how we do business.

Cloud is becoming integral to government transformation

Start with a trusted & resilient foundation	Reshape how you engage with citizens
Leverage economies of scale and expertise	Enable more productive work
Use the cloud to drive future technology uptake	Enable domestic IoT economy



Cloud Policy Principles

The six principles provide a framework for government ICT decision-makers and have been designed to provide helpful guidance to policy makers as well as ministries and various departments as they begin to implement procurement guidelines for cloud computing. Ultimately, these six principles create a foundational framework that governments can utilize as they develop 21st century policies to transform government, advance the security and resiliency of their services, and spark more innovative digital societies.

Innovative

Cloud policies should set a clear path toward innovating and advancing the security and resiliency of their government services.

While the pace at which governments incorporate new technologies must be responsive to the realities of their environments, Microsoft encourages governments to take a forward-leaning approach, empowering organizations to move to the cloud when appropriate by adopting a "cloud first" policy.

Flexible

Cloud policies should be flexible and should enable governments to select the most suitable cloud types for delivering their services in a secure and resilient manner.

Government entities should retain sufficient flexibility as they develop and implement their cloud security policies and evaluate various cloud deployment and service models, ensuring that they can apply their knowledge and hands-on experience to make the best decisions for their environments.

Data aware

Cloud policies should demonstrate data awareness by ensuring that assessments, categorization, and protection of data are commensurate with risk.

Governments should take a conscious approach to data governance, categorizing their systems and data by sensitivity and business impact, which will enable them to realize optimizations and compliance efficiencies that might not be possible when all data is assigned the same value.

Risk-based

Cloud policies should prioritize the assessment, management, and reduction of risk in the delivery of cloud services for governments.

Governments should assess risks in cloud and in on-premises technologies, determining how their risk profiles may improve by migrating to the cloud as well as what net new risks must be managed, and should distinguish between common and unique risks, easing later risk management decisions.

Standard-based

Cloud policies should leverage global standards as the basic requirements for increasing security and resiliency in government cloud services.

Because many governments share common risks and cloud computing is based on aggregation and scale to drive down costs, governments should leverage global standards as the basis of their cloud security certifications, enabling greater efficiency, lower costs, and more market competition.

Transparent

Cloud policies should establish transparent and trusted processes for developing compliance requirements and for evaluating the security and resiliency of cloud services.

Governments should leverage the expertise and perspectives of all relevant stakeholders when developing cloud requirements, enabling them to establish clear, comprehensive, and easily adoptable compliance frameworks, and utilize clear evaluative criteria in assessing cloud providers.

Read the full paper: Transforming Governments

For more information please go to: http://www.microsoft.com/cybersecurity