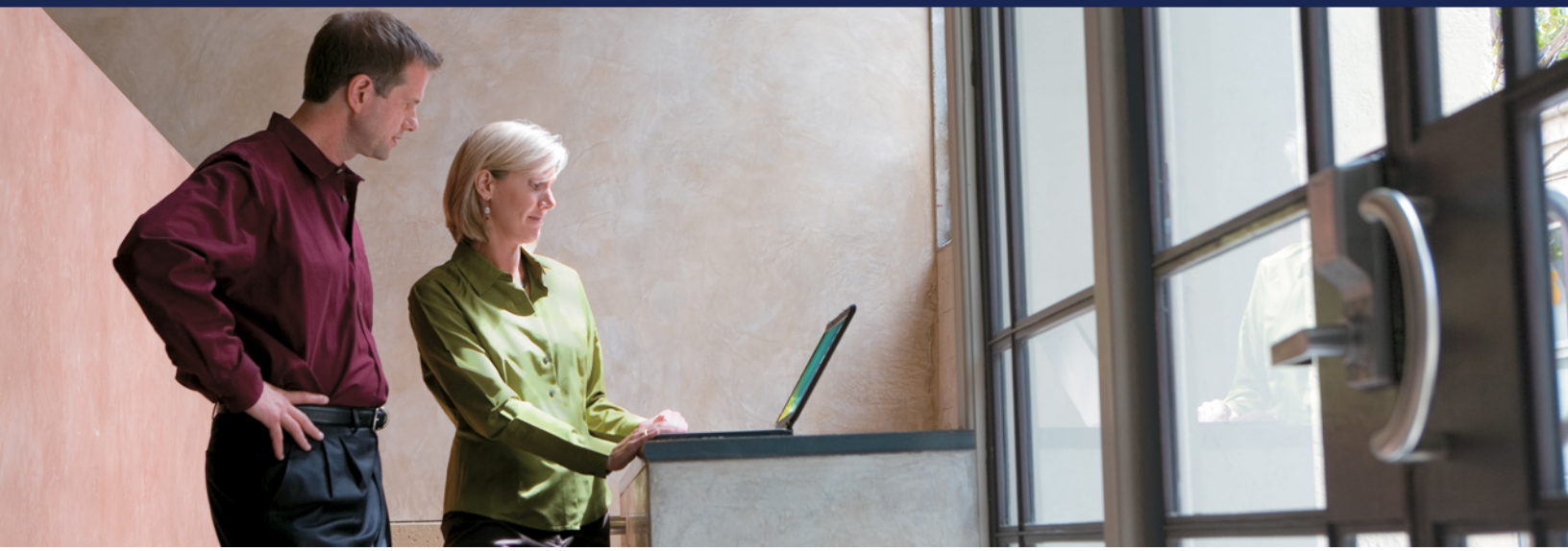
Microsoft

Trustworthy Computing



Privacy in the Public Cloud: The Office 365 Approach

December 2011

© 2011 Microsoft Corporation. All rights reserved. This document is provided “as is.” Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Contents

Introduction

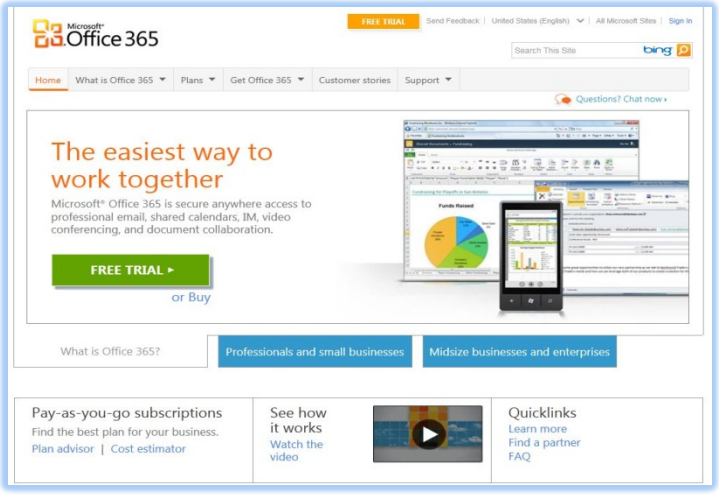
Since our 2010 whitepaper "Privacy in the Cloud," awareness and adoption of cloud computing have continued to increase. Global enterprises and entrepreneurs alike are turning to the cloud to accelerate innovation, launch new businesses, and cut costs. Government agencies, public service providers, and educational institutions are migrating to the cloud to better serve constituents and reduce IT spending, particularly in response to shrinking budgets.

But not all the news has been positive. Hacking attacks, theft, and misuse of data managed by online service providers have raised questions about the privacy and security of cloud computing.

For some large enterprises with highly sensitive data, such incidents have increased the appeal of private cloud solutions. Indeed, a "one-size-fits-all" approach may not be appropriate for governments or large organizations with many different classes of data, and private or hybrid cloud solutions that allow customers to keep selected data on premises can make good sense for those with specialized data protection requirements. Microsoft offers a full menu of private cloud solutions, and we recently published a whitepaper titled "Microsoft Private Cloud: A comparative look at Functionality, Benefits, and Economics."

But private clouds dedicate significant computing resources to just one or a handful of customers, so they can be cost-prohibitive for many businesses and public-sector agencies that are anxious to reap the benefits of cloud computing.

Consequently, we expect public cloud services—which use advanced, multi-tenant data centers[1] to provide highly scalable and affordable computing services to thousands of customers simultaneously—to be the most popular cloud computing model for the foreseeable future.[2]



Still, the growth of public cloud services is not inevitable. Microsoft understands that unless we are responsive to customers' and regulators' questions about data protection in public clouds, we will not earn the trust that is necessary for our cloud services to satisfy our customers' needs.

This is why data protection figures prominently in Office 365, Microsoft's newest cloud-based productivity service.

---

[1] "Microsoft Expands Cloud Computing Capabilities & Services in Europe." Microsoft press release, Sept. 2009.

[2] "The Economics of the Cloud." Microsoft whitepaper, Nov. 2010.

Reflecting Microsoft's approach to privacy by design, Office 365 was built from the ground up with strong data protection in mind.

In the following pages, we will discuss Microsoft's philosophical and practical approach to safeguarding information in the cloud, and we will describe several of the tangible benefits that have resulted for Office 365 customers.

Privacy at Microsoft

As part of our long-term commitment to Trustworthy Computing, Microsoft strives to earn and strengthen trust by building robust privacy and data protections into our products and services. We work to responsibly manage and protect the data we store, be transparent about our privacy practices, and offer meaningful privacy choices. These three tenets—responsibility, transparency, and choice—are the foundation of Microsoft's approach to privacy.

Our privacy principles and our internal privacy standards guide the collection and use of customer and partner information at Microsoft and give our employees a clear framework to help ensure that we manage data responsibly.

To put our principles and standards into practice, we have invested heavily to build a comprehensive privacy governance program. Microsoft employs more than 40 full-time privacy professionals, with several hundred other employees helping to ensure that privacy policies, procedures, and technologies are applied across our products and services.

When it comes to cloud computing, Microsoft has been addressing privacy issues associated with online services since the launch of the MSN network in 1994. Today, we manage a cloud-based infrastructure that supports more than 200 online services and websites that attract more than 600 million unique users worldwide each month.

We recognize that cloud services often raise unique security and privacy questions for business, education, and government customers, so we have adapted our policies and governance programs to address customer concerns, facilitate regulatory compliance, and build greater trust in cloud computing.

For example, we contractually commit to specific data handling processes as part of our agreements for popular cloud services such as Microsoft Exchange Online, SharePoint Online, and Lync Online. We also provide customers with flexible management tools that help protect sensitive data and support compliance with government privacy and security guidelines.

Such transparent policies and strong tools are essential for our customers as they deal with the privacy and security questions that arise from their use of cloud services.

The Office 365 Privacy Opportunity

Microsoft helped usher in the era of enterprise cloud computing in 2008 when Bill Gates announced that the company would offer online versions of its popular Exchange Server and SharePoint Server software for businesses of all sizes. The services, which in 2009 became part of the Microsoft Business Productivity Online Suite (BPOS), gave thousands of global businesses their first taste of cloud computing by providing access to email, calendaring, and shared workspaces over the Internet.

But because this first generation of "software-as-a-service" cloud offerings had its roots in traditional server software, it was not fully optimized to take advantage of Microsoft's global network of technologically advanced data centers.

Microsoft Office 365 delivers the power of cloud productivity to businesses of all sizes, helping them to save time and money and free up valued resources. Office 365 supplements the familiar Office desktop suite—which includes such popular programs as Microsoft Word, Excel, and Outlook—with cloud-based versions of these programs as well as our next-generation communications and collaboration services: Exchange Online, SharePoint Online, and Lync Online.

So, even as BPOS was launching, Microsoft was laying the groundwork for its successor: Office 365. The multi-year development effort, which culminated in the global launch of Office 365 in June 2011, yielded an online business service purposely built to optimize the flexibility, responsiveness, and efficiency of the cloud.

Office 365 was also built with an emphasis on strong data protection. Reflecting Microsoft's approach to privacy by design, a team of privacy professionals was dedicated to the product early in the development cycle and worked in close partnership with engineers, business planners, and marketers. Consequently, privacy has been an integral part of Office 365 from the beginning, not an afterthought. In addition, employees distributed throughout the organization are accountable for managing the service's privacy and security risks.

The result is an enterprise cloud service with robust data protections that reflect Microsoft's core privacy tenets of responsibility, transparency, and choice.

Responsibility

We understand that managing customer information is a responsibility that includes important security and privacy obligations. This is particularly true for cloud-based services such as Office 365. We have a broad network of people and processes that implement our privacy standards and provide privacy guidance and training. If a privacy incident occurs, we have rigorous procedures to address the problem, diagnose the cause, and update customers in a timely manner.

A few highlights of our approach to privacy governance in Office 365 are outlined below.

Standing the Test of Time

Criteria for determining appropriate levels of privacy and security in the cloud are changing rapidly. What matters most today may be a low priority tomorrow. As a result, when evaluating a cloud provider,

organizations would be wise to consider the depth and breadth of the provider's governance model and its ability to quickly adapt to changing privacy priorities.

With Office 365, we have employed a variety of risk management mechanisms to appropriately manage regulatory change, organizational change, personnel change, and technological change.

Before any of the services that are part of Office 365 launch to the public, subject-matter experts conduct privacy, security, and business continuity risk assessments on each service and work closely with the service owners to remediate any identified risks.

After launch, we use a process of continuous monitoring that we call the Trustworthy Services Lifecycle to ensure that our data protection systems are functioning properly. We test required functionality annually, semi-annually, quarterly, monthly, or at the time of each new release, depending on the level of risk associated with the particular privacy or security control.

We conduct regular risk assessments to refresh the control framework and, if necessary, to reset priorities if new aspects of the service emerge as high-risk.

This multi-layered and continuous approach to monitoring the Office 365 data protection environment helps us quickly diagnose and remedy problems that occur and helps our customers respond quickly to shifting regulatory or industry requirements.

Enabling Regulatory Compliance

Just as Microsoft has a responsibility to process our enterprise customers' information in a trustworthy manner, many of our customers have a responsibility to comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data.

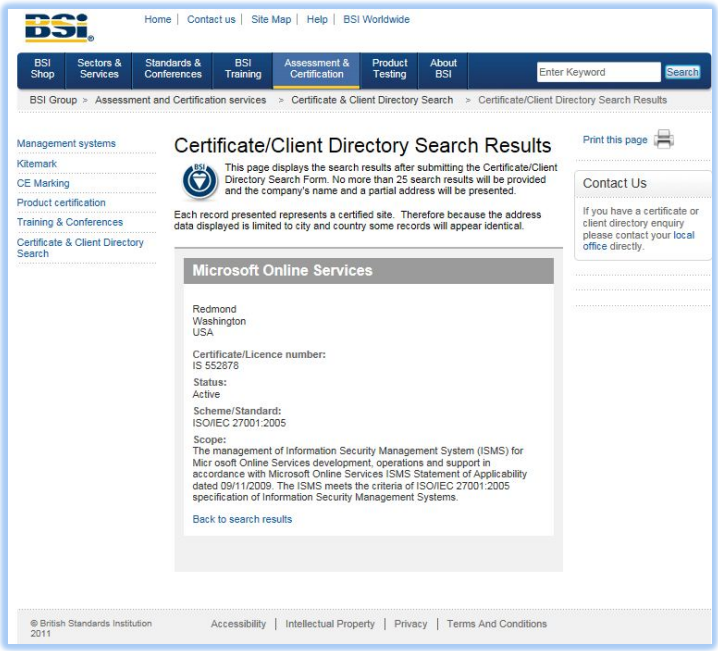
As a provider of global cloud services, we must run our services with common operational practices and features that span multiple customers and jurisdictions. To fulfill our privacy responsibility to our customers as well as help our diverse customer base fulfill its regulatory obligations, we set the bar high and then build our services to meet that bar using common privacy and security controls.

While it is ultimately up to our customers to determine whether our services satisfy their specific regulatory needs, we are committed to providing detailed information about our cloud services to help them in their assessments.

One tool we have developed to facilitate customers' assessments of Office 365 is the Office 365 Trust Center, an online repository of detailed information about Office 365 privacy and security practices. For example, on the Regulatory Compliance page of the Trust Center, we explain how we believe Office 365 helps facilitate compliance with a range of major statutes, from European Union data protection laws to the U.S. Gramm-Leach-Bliley Act, which includes provisions on the protection of consumers' financial information.

Another resource we offer to help customers evaluate Office 365 is detailed information about the well-recognized certifications that the service has attained. On the Security, Audits, and Certifications page of the Trust Center, customers can locate information about the certifications held by both Office 365 and the Microsoft data centers that host the service. By making this information readily available, we empower

customers to validate that what we say about our security and privacy practices has been affirmed by an accredited third party.



One compliance framework in particular—the highly regarded ISO/IEC 27001 standard for information security management systems—forms the foundation of our security and privacy approach with Office 365 and its supporting infrastructure. ISO/IEC 27001 is one of the most widely recognized certifications for a cloud service, and thus one of the most valued by our customers.

In addition to having our independent auditor, the British Standards Institute (BSI), verify the compliance of Office 365 with ISO/IEC 27001, we have asked BSI to review more than 20 additional privacy controls that we built into the service to better align it with comprehensive European data protection regulations. We have taken this unique approach to help our European customers understand the protections we have put in place to help them satisfy the specific expectations of both European citizens and European regulators.

The full results of BSI's findings are included in its ISO/IEC 27001 audit report on Office 365, a summary of which is available to Office 365 customers upon request.

Support for EU Model Clauses

In another effort to accommodate the data protection demands of European entities, Office 365 offers the opportunity for customers with European users to sign data processing agreements with the standard contractual clauses published by the European Commission.

European law prohibits companies from transferring personal data from the EU except under specific conditions. One way to transfer such data is to procure cloud services from companies that abide by the U.S.-EU Safe Harbor Framework. However, EU companies may want the more stringent protections of a detailed data processing agreement and the standard contractual clauses published by the European Commission, which are known as the EU Model Clauses. Microsoft's willingness to sign these agreements means that Microsoft contractually guarantees that Office 365 will follow the stringent privacy and security standards detailed in the Model Clauses.

Using Customer Data Only for the Customers' Purposes

Responsible cloud providers must have strong internal policies in place that clearly delineate what the provider and its partners can and cannot do with customer information.

In Office 365, we use our customers' data only for what they pay us for—to maintain and provide Office 365 services. As part of providing a quality service, we will troubleshoot in order to prevent, identify, or repair problems and to improve features that protect our customers. But Office 365 does not build advertising products out of our customers' data. We also don't scan our customers' email or documents for the purpose of building analytics, data mining, advertising, or improving the service without our customers' permission. In addition, Office 365 allows customers to keep their data separate from Microsoft's consumer services.

Controlling Access to Customer Data

Office 365 applies strict controls over who will be granted access to key customer data. Microsoft and vendor support personnel are required to have a legitimate business justification to request access to Office 365 customers' core data, and the request must be approved by the person's manager prior to gaining access. In addition, access levels are reviewed on a periodic basis to ensure that only Microsoft employees or support personnel who have an appropriate business justification have access to the systems.

Further, all Office 365 support personnel are accountable for their handling of customer data. Accountability is enforced through a set of system controls, including the use of unique user names, data access controls, and auditing. Unlike generic user names such as "Guest" or "Administrator," unique names connect the use of customer data to specific individuals.

For a detailed breakdown of how we handle specific classes of data stored and generated by users of Office 365, see the Data Use Limits page of the Office 365 Trust Center (which is discussed in more detail below).

Securing Customer Information and Office 365 Systems

According to a popular maxim in IT circles, "You can have security without privacy, but you can't have privacy without security." This statement certainly applies to public cloud computing, where customers rely on online service providers such as Microsoft not only to securely store their data but also to keep it safe from loss, theft, or misuse by third parties, other customers, or even the provider's employees.

We understand that robust physical and logical security is a prerequisite for any successful privacy program, and we protect Office 365 using a comprehensive security regimen that is monitored 24/7 and updated regularly.

Unlike on-premises software that lives behind a corporate firewall and can be accessed only over a virtual private network, Office 365 is designed specifically for secure access over the Internet.

Office 365 provides anti-spam and anti-malware technologies that are automatically updated to protect against the latest threats. The security features and services associated with Office 365 are built in, reducing customers' time and cost associated with securing their IT systems. At the same time, Office 365 enables customers to easily control permissions, policies, and features through online administration and management consoles to meet their specific security needs.

For most customers, Office 365 is a multi-tenant, public cloud service. That means one customer's data may be stored on the same hardware as several other customers' data. This is one reason Office 365 can provide the cost and scalability benefits it does. Microsoft goes to great lengths to ensure that the multi-tenant architecture

of Office 365 supports enterprise privacy and security requirements, and we logically segregate data storage and processing for different customers through specialized technology engineered specifically for the purpose.

Our data centers are designed, built, and managed using a "defense-in-depth" strategy at both the physical and logical layers, and our services are engineered to be secure using Microsoft's Security Development Lifecycle.

All Office 365 data centers have biometric access controls, and most require palm prints to gain entry. In addition, physical access to most data centers is controlled by two-tier authentication that includes both proxy card access readers and hand geometry biometric readers.

For more on security in Office 365 and the Microsoft data centers that host it, please see the "Security in Office 365" whitepaper and our Global Foundation Services website.

Transparency

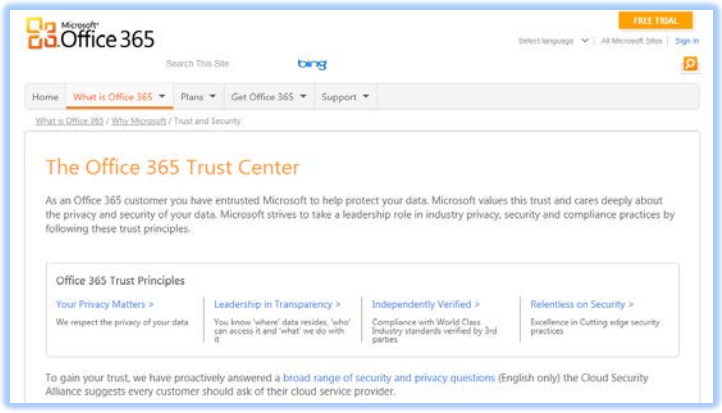
Although many organizations cite privacy and security concerns as major obstacles to their adoption of cloud services, information on the privacy and security practices of many cloud providers is either difficult to find or indecipherable to all but the most astute IT professionals.

To help our customers find answers to their privacy and security questions about Office 365, we strive to be as transparent as possible about our data protection policies and procedures.

The Office 365 Trust Center

The centerpiece of our transparency effort with Office 365 is the Office 365 Trust Center, which launched in conjunction with the cloud service in June 2011 and was updated in December 2011.

The aim of the Trust Center is to tell customers, in plain language, exactly how we handle and use data gathered in their interactions with Office 365.



The site details commitments we make to Office 365 customers in six key privacy areas: Data Use Limits; Administrative Access; Geographic Boundaries; Third Parties; Security, Audits, and Certifications; and Regulatory Compliance.

The Trust Center also includes links to tools that customers can use to stay current with changes to Office 365 security and privacy practices, to help ensure ongoing regulatory compliance, and to obtain more detailed information about the specific privacy and security practices of the individual services that comprise Office 365 (such as Exchange Online, SharePoint Online, and Lync Online).

Just as Office 365 will be a continuously evolving and improving service, the Trust Center will be a living resource that customers can use to stay abreast of the most current and accurate information available about privacy and security practices in Office 365.

Geographic Boundaries

One of the most common questions asked of cloud providers is also one of the simplest: "Where is my data?" With Office 365, we provide a thorough summary of our data location strategy on the Geographic Boundaries page of the Trust Center.

This page describes where Microsoft stores and accesses customer data in the course of providing the Office 365 service. Microsoft has a regionalized data center strategy. The specific details of where data is located or accessed from depend on the customer's ship-to address, which the customer provides when purchasing the service. The three regions are the Americas, Asia, and Europe.

The Geographic Boundaries page also outlines the steps we take to ensure that information is not lost if the power fails in one data center. All such data is backed up in one or more data centers in another country or region.

Third Parties

Another frequent topic of concern is third-party access to cloud data. Many customers worry that beyond the cloud service provider they purchase services from directly, an unseen web of subcontractors, vendors, and other third parties may be improperly accessing, reviewing, and using their information.

Microsoft readily acknowledges that it relies on partners and subcontractors to ensure that Office 365 performs optimally for all of our customers, no matter where they are. But we think our customers should be able to know not only what kinds of privacy and security minimums we expect of such third parties, but also who the third parties are.

This is why we publish such information on the Third Parties page of the Trust Center. The page links to a current list of Office 365 subcontractors and provides information on how Microsoft works to help ensure that subcontractors comply with our privacy requirements. Subcontractors that work in facilities or on equipment controlled by Microsoft must follow our privacy standards, and all other subcontractors must follow privacy standards equivalent to our own.

Comparing Cloud Provider Controls and Policies

To help potential customers evaluate different cloud service providers, the not-for-profit Cloud Security Alliance (CSA) developed a set of security and privacy criteria called the Cloud Controls Matrix that customers can use to compare and contrast different providers' data protection controls and information about their policies across 13 domains.

To help enable such comparisons of Office 365, Microsoft developed a 50-page whitepaper that details how Office 365 fulfills the security, privacy, compliance, and risk management requirements defined in the Cloud Controls Matrix.

The paper is available on the Office 365 website and is also available for download in the CSA's searchable Security, Trust & Assurance Registry, which allows potential cloud customers to quickly access information on a variety of cloud providers.

Choice

We believe that customers want clear opportunities to choose whether their information will be collected, shared, or made public. This includes the flexibility to limit or eliminate information sharing or to set different levels of access.

For business, government, and education customers, choice means having tools to maintain and control access to the information stored in their cloud accounts. Microsoft has developed a number of tools for administrators within customer organizations to control access to Office 365.

Administrative Access

In formulating our strategy for administrative access to data managed by Office 365, we worked with three priorities in mind:

- We always give customers access to their customer data.
- Access to customer data is strictly limited, and sample audits are performed by both Microsoft and third parties to verify that access is only for appropriate business purposes.
- We recognize the extra importance of our customers' core data, such as the body of Exchange Online emails and SharePoint Online team site content. If anyone—whether Microsoft personnel, partner personnel, or a customer's own administrator—accesses core data on the service, we can provide a report on that access upon request.

With Office 365, customers have complete access to their own environment, including user mail boxes, SharePoint websites, and document stores. The customer maintains control over security policies and user accounts. This degree of control enables administrators to effectively enforce their organization's privacy and security policies. Policies and users can be managed using a web-based management console or remote PowerShell for automation of routine tasks.

Identity Management

Office 365 provides two options for user identification: Microsoft Office 365 user IDs and federated IDs. In the first case, administrators create Office 365 user IDs for each of their organization's individual users of Office 365. Users sign in to all of their Office 365 services using a single login and password. A single sign-in application helps users easily create and use strong passwords that help keep their information safe.

Alternatively, customers can choose federated identification, which uses on-premises Active Directory Federation Services (a service of Microsoft Windows Server 2008) to authenticate users on Office 365 using their existing corporate ID and password. In this scenario, identities are administered only on premises. This enables organizations to use two-factor authentication (such as smart cards or biometrics in addition to passwords) for maximum security.

Microsoft Partners

Lastly, Microsoft provides customers and their administrators with a number of ways to initiate, maintain, or terminate relationships with Microsoft partners who are part of the Office 365 ecosystem.

We recognize that one compelling aspect of Office 365 is the number of partners that can provide additional services that our customers may want. For instance, some customers may hire a Microsoft support partner to administer their Office 365 services for them. To assist in maintaining security and privacy while taking advantage of our network of partners, we provide tools that enable Office 365 customers to monitor and quickly disable partners' access to their information at any time, without having to disable the underlying Office 365 account.

Conclusion

Many public and private organizations around the world are already enjoying the efficiency, flexibility, and cost savings that cloud computing can provide. Yet some are waiting to move to the cloud until they have greater trust that their information will remain private and secure. Because Microsoft recognizes that privacy and security are major concerns for cloud customers, we developed our latest cloud-based productivity service, Office 365, from the ground up with strong data protection in mind. Additional information on Office 365 can be found at www.Office365.com, and additional information on Microsoft's approach to privacy is available at www.microsoft.com/privacy.

Additional Information

"Privacy in the Cloud," Microsoft whitepaper

"The Economics of the Cloud," Microsoft whitepaper

"Security in Office 365," Microsoft whitepaper

Office 365 FAQ website

Office 365 Trust Center website

Microsoft Global Foundation Services website