Microsoft

Security and Compliance

Office 365

Published: May 2014

For the latest information, please visit the Office 365 Trust Center at
http://trust.office365.com

Introduction 1

Service-Level Security 2

- Physical layer—facility and network security 4
- Logical layer—host, application, admin user 5
- Data layer—data 7
- Data integrity and encryption 7
- Protection from security threats 8
- Security monitoring and response 9
- Independent verification 9

Security Customer Controls 10

- Secure end-user access 12

Privacy by Design 14

Privacy Customer Controls 15

Service Compliance 16

Customer Compliance Controls 18

Conclusion 21

Introduction

Information security is an essential consideration for all IT organizations around the world. In addition to the prevalence of information technology, the complexity of delivering access to services from a growing number of devices, platforms, and places than ever before forces information security to be a paramount matter. Multi-device access benefits your users, especially with the consumerization of IT, but broader access represents another potential attack surface. At the same time, organizations face ever-evolving cyber-threats from around the world that target users who may accidentally lose or compromise sensitive data.

When you consider moving your organization to cloud services to store your data and various productivity services, the security concerns add another layer of consideration. That consideration is one of trust. You have to be able to trust your service provider to take care of the key expectations around processing and managing your data - security, privacy and compliance.

Our construct for security, compliance, and privacy for Office 365 has two equally important dimensions. The first dimension includes service-level capabilities that include technology, operational procedures, and policies that are enabled by default for customers using the service. The second entails customer controls that include features that enable you to customize your Office 365 environment based on the specific needs of your organization.

Security in Office 365 is an ongoing process, not a steady state. It is constantly maintained, enhanced, and verified by highly skilled, experienced and trained personnel. We strive to keep software and hardware technologies up to date and refined through robust designing, building, operating, and supporting processes. To help keep Office 365 security at the top of the industry, we use processes such as the Security Development Lifecycle; traffic throttling; and preventing, detecting, and mitigating breach. To learn more and stay up-to-date with Office 365 security and compliance, you can visit the Office 365 trust center.

Service-Level Security

We have been recognized as an industry leader in cloud security with policies and controls for even the most sophisticated organizations. Using decades of experience building enterprise software and running online services, our team is constantly learning and continuously updating the service to deliver a highly secure cloud productivity service that meets rigorous industry standards in compliance.

At the service level, we use a defense in depth strategy that protects your data through layers of security (at the physical, logical and data layers) in the service.

At a high level, the layers of defense can be visualized as:

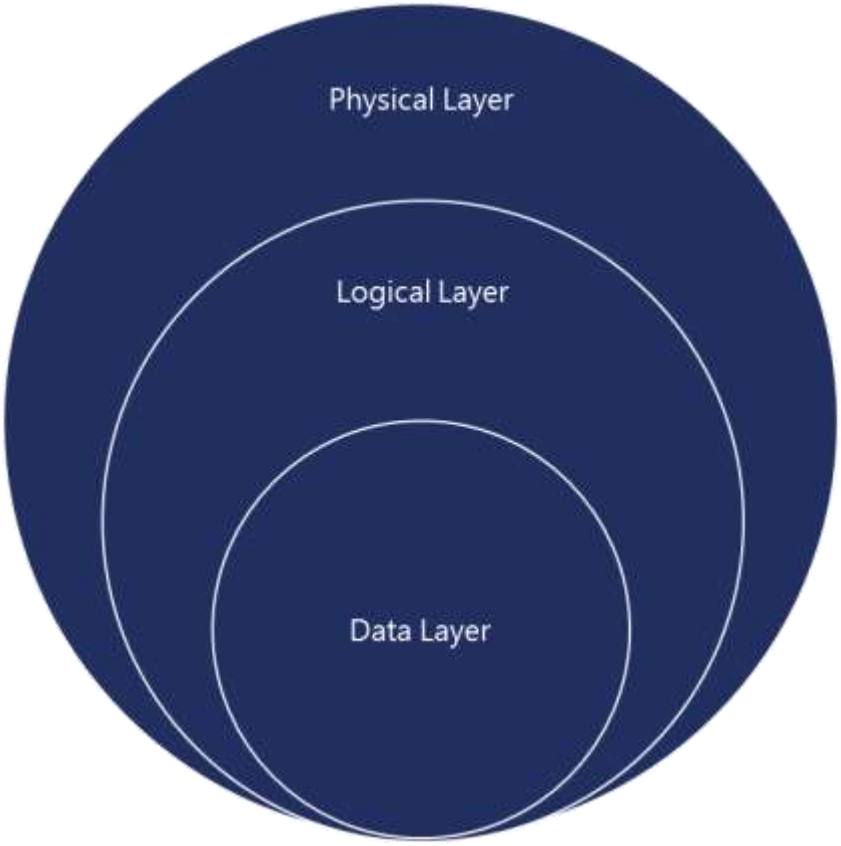

Figure 1 Defense in depth

A defense-in-depth strategy assures that security controls are present at various layers of the service and ensures that should any one area fail there are compensating controls to maintain security at all times.

The strategy also includes tactics to detect, prevent, and mitigate a security breach before it happens. This involves continuous improvements to service-level security features, including:

- Port scanning and remediation
- Perimeter vulnerability scanning
- Operating system security patching
- Network-level DDOS (distributed denial-of-service) detection and prevention
- Multi-factor authentication for service access

With regards to people and process, preventing breach involves:

- Auditing all operator/administrator access and actions
- Zero standing permission for administrators in the service
- "Just-In-Time (JIT) access and elevation" (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) to troubleshoot the service
- Segregation of the employee email environment from the production access environment
- Mandatory background checks for high privilege access. These checks are a highly scrutinized, manual-approval process.

Preventing breach also involves automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration. Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services.

We continue to invest in systems automation that helps identify abnormal and suspicious behavior and respond quickly to mitigate security risk. We are also continuously evolving a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service. We regularly conduct penetration tests to enable continuous improvement of incident response procedures. These internal tests help our security experts create a methodical, repeatable, and optimized stepwise response process and automation.

Physical layer—facility and network security

Facility

Customer data is stored in our Office 365 data centers that are geographically distributed while taking regional data location considerations into account. Our data centers are built from the ground up to protect services and data from harm by natural disaster or unauthorized access. Data center access is restricted 24 hours a day by job function—with only customer application and services access given to essential personnel. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication. The data centers are monitored using motion sensors, video surveillance, and security breach alarms. In case of a natural disaster, security also includes automated fire prevention and extinguishing systems and seismically braced racks where necessary.

Network

Perimeter protection is implemented through the use of controlled devices at the network edge and on points throughout the network. The overarching principle of our network security is to allow only connections and communications that are necessary to allow systems to operate, blocking all other ports, protocols and connections. Access Control Lists (ACLs) implemented in the form of tiered ACLs on routers, IPsec policies on hosts, firewall rules and host based firewall rules are implemented in the network with restrictions on network communication, protocols, and port numbers. Edge router security allows the ability to detect intrusions and signs of vulnerability at the network layer. Networks within the Office 365 data centers are further segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces.

Logical layer—host, application, admin user

The logical layer of security involves many controls and processes implemented to secure the host machines, applications running on those hosts and from administrators that may perform any work on those host machines and applications.

Automated operations

Most of the operations performed on hosts and applications by administrators are automated so that human intervention is reduced to a minimum, reducing the possibility of an inconsistent configuration or a malicious activity. This automated approach extends to the deployment of systems within our data centers.

Admin access to data

Administrator access to Office 365 and your data is strictly controlled. Core tenets of this process are role based access and granting personnel least privilege access to the service that is necessary to perform specific operations. These tenets are followed whether the access is physical (i.e., to the data center or the servers) or logical. An example where this comes to life is a process called "lockbox' that administrators use to request access for elevated privileges.

Access control happens at various levels:

1. Personnel level to ensure that there are appropriate background checks and strict account management so that only those essential to the task may perform the task
2. Role based access control
3. A "lock box" process which allows:
    a. Just-in-time accounts with high entropy passwords
    b. Access for a limited amount of time
    c. Access to take specific actions based on the role
4. The servers in the Office 365 service have a pre-determined set of processes that can be run using Applocker.
5. Auditing and review of all access

Security development life cycle

The Microsoft Security Development Lifecycle (SDL) is a comprehensive security assurance process that informs every stage of design, development, and deployment of our software and services, including Office 365. Through design requirements, analysis of attack surface, and threat modeling, the SDL helps us predict, identify, and mitigate vulnerabilities and threats from before a service is launched through its entire

itlockerproduction life cycle. We continuously update the SDL using the latest data and best practices to help ensure that new services and software associated with Office 365 are highly secure from day one.

Anti-malware, patching, and configuration management

The use of anti-malware software is a principal mechanism for protection of your assets in Office 365 from malicious software. The software detects and prevents the introduction of computer viruses and worms into the service systems. It also quarantines infected systems and prevents further damage until remediation steps are taken. Anti-malware software provides both preventive and detective control over malicious software.

Our standard baseline configuration requirements for servers, network devices, and other Microsoft applications are documented where the standards outline the use of a standard package. These packages are pretested and configured with security controls.

Changes, such as updates, hotfixes, and patches made to the production environment, follow the same standard change management process. Patches are implemented within the time frame specified by the issuing company. Changes are both reviewed and evaluated by our review teams and the Change Advisory Board for applicability, risk, and resource assignment prior to being implemented.

Data layer—data

Office 365 is a highly scalable multi-tenant service, which means that your data securely shares the some of the same hardware resources as other customers. We have designed Office 365 to host multiple customers in the service in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through Active Directory and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Active Directory isolates your data using security boundaries. This safeguards your data so that the data cannot be accessed or compromised by co-tenants.

Data integrity and encryption

Our Office 365 services follow industry cryptographic standards such as SSL/TLS (Secure Sockets Layer / Transport Layer Security), AES etc. to protect confidentiality and integrity of data.

All customer-facing servers negotiate a secure session using SSL/TLS (Secure Sockets Layer / Transport Layer Security) with client machines so as to secure the data in transit. This applies to various protocols such as HTTP(S), POP3, etc. that are used by clients such as Lync, Outlook and Outlook Web App (OWA) on any device. Microsoft is working to support and deploy strong encryption using SSLv3.0 support and TLSv1.1/1.2 across all workloads. The use of TLS/SSL establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the data center.

To further protect your data in the Office 365 service, we use BitLocker as one mechanism to encrypt your data at rest. BitLocker is either deployed with Advanced Encryption Standard (AES) 128bit or AES 256bit encryption on servers that hold all messaging data including emails and IM conversations, content stored in SharePoint Online and OneDrive for Business. BitLocker drive encryption is a data protection feature that is integrated with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers and disks.

In certain other scenarios as appropriate, we use file level encryption. For example, when files and presentations are uploaded by meeting participants, this content is encrypted using 128 bit AES encryption by the Lync Online web conferencing server.

Our latest encryption feature with which content in OneDrive for Business and SharePoint Online will be encrypted at rest is called *Per-file encryption*. With this, the encryption technology in Office 365 moves beyond a single encryption key per disk to deliver a unique encryption key per file. With this technology, every file stored in SharePoint Online—including OneDrive for Business folders—is encrypted with its own key, and subsequent updates to the file are encrypted with their own unique key as well. Your organization's files will be distributed across multiple Microsoft Azure Storage containers, each with separate credentials, rather than storing them all in a single database. By spreading encrypted files across storage locations, encrypting the map of file locations itself, and physically separating master encryption keys from both content

and the file map, this new encryption storage technology makes OneDrive for Business and SharePoint Online a highly secure environment for your data.

Protection from security threats

Threat management strategy for Office 365 is a composite of identifying a potential threats intent, capability, and probability of successful exploitation of a vulnerability. The controls used to safe guard against such exploitations are heavily founded upon security standards. By validating the ISO 27001/27002 and NIST 800-53 controls implemented by Microsoft via the independent audits of these controls, you are able to assess the effectiveness of the controls deployed by us.

The overall cyber threat landscape has evolved from traditional opportunistic threats to also include persistent and determined adversaries. We equips you with a defense-in-depth approach to address the continuum of threats ranging from common "hacktivists" to cyber criminals to nation-state actors.

Our Office 365 security strategy is founded upon a dynamic strategy with four pillars of thought. The mindset shift we made to make our defenses more effective and ever evolving is commonly referred to as "Assume Breach" and assumes that a breach has already happened in the environment and is simply not known. With this mindset, the security teams are continuously attempting to detect and mitigate security threats that are not widely known. One set of exercises is to artificially propagate a security threat and have another group respond and mitigate the threat. The primary goal of these exercises is to make Office 365 resilient so the new vulnerabilities are quickly detected and mitigated.

The first pillar of the security strategy is referred to as "Prevent Breach." Our investment in this pillar involves continuous improvements to built-in security features. These include port scanning and remediation, perimeter vulnerability scanning, operating system patches, network level Isolation/breach boundaries, DDoS (Distributed Denial of Service) detection and prevention, just-in-time access, live site penetration testing, and multi-factor authentication for service access.

The second pillar is referred to as "Detect Breach." In this pillar, our system and security alerts are harvested and correlated via a massive internal analysis system. The signals analyze alerts that are internal to the system as well as external signals (for example coming from customer incidents). Based on machine learning, we can quickly incorporate new patterns to trigger alerts, as well as automatically trigger alerts on anomalies in the system.

The third pillar is referred to as "Respond to Breach." This pillar is used to mitigate the effects if a component is compromised. A diligent incident response process, standard operating procedures in case of an incident, ability to deny or stop access to sensitive data and identification tools to promptly identify involved parties helps ensure that the mitigation is successful.

The fourth pillar is referred to as "Recover from Breach," which includes the standard operating procedures to return the service to operations. The pillar includes the ability to

change the security principals in the environment, automatically update the affected systems, and audit the state of the deployment to identify any anomalies.

Security monitoring and response

Many threats target software vulnerabilities, but others attack operational weaknesses, which is why Microsoft uses the Operational Security Assurance (OSA) framework. OSA supports continuous monitoring, helps to identify operational risks, provides operational security guidelines, and validates that those guidelines are followed. OSA helps make Microsoft cloud infrastructure more resilient to attack by decreasing the amount of time needed to protect, detect, and respond to security threats.

Independent verification

Office 365 has operationalized security into a scalable process that can quickly adapt to security trends and industry-specific needs. Microsoft engages in regular risk management reviews, and it develops and maintains a security control framework that meets the latest standards. Internal reviews and external audits by trusted organizations are incorporated into the Office 365 service life cycle. Close working relationships with other Microsoft teams result in a comprehensive approach to securing applications in the cloud.

Key standards that give you confidence in Microsoft's security technologies and best practices are independent audits and verifications of adherence to standards embodied in ISO 27001, SSAE 16 SOC1 Type II and HIPAA.

Security Customer Controls

Office 365 combines the familiar Microsoft Office suite with cloud-based versions of our next-generation communications and collaboration services: Exchange Online, SharePoint Online, and Lync Online. Each of these services offers individualized security features that you can control. These controls allow you to help adhere to compliance requirements, give access to services and content to individuals in your organization, configure anti-malware / anti-spam controls, and encrypt data.

Data integrity and encryption

Along with the encryption technologies that are addressed at the service-level in Office 365 and managed by Microsoft, Microsoft also offers various technologies that you can implement and configure in your Office 365 tenant. These technologies offer a variety of ways to encrypt data in different workloads and offer ways to encrypt data at rest or in transit. These technologies are as follows:

- Rights Management Service
- Secure Multipurpose Internet Mail Extension (S/MIME)
- Office 365 Message Encryption
- Transport Layer Security (TLS) for SMTP messages to partners

Rights Management Service

Rights Management Service (RMS) is a unique technology that provides best-in-class data protection at the file level. With RMS you can not only encrypt data but also apply policies on the data to limit or allow the actions by the recipient of the data. You can read the blog here to understand how to use RMS to collaborate securely.

RMS can be deployed in two forms:

- *AD RMS*—an on-premises implementation
- *Azure RMS*—a cloud-based offering of RMS. Azure RMS comes with Office 365 and can be deployed for an entire organization with a few clicks. Details on Azure RMS can be found at http://technet.microsoft.com/en-us/library/jj585016.aspx.

With effective use of Azure RMS while sharing sensitive data, you can reduce the security risks due to wire-tapping, man-in-the-middle attack, and more. At the same time, you can also prevent any unwarranted access of data (for example, emails and files) in transit or at rest by an unauthorized user who does not have appropriate permissions via policies that are embedded in metadata, mitigating the risk of a data loss or breach.

Secure Multipurpose Internet Mail Extension

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and digital signing of MIME data.

S/MIME allows a user to (1) encrypt an email (2) digitally sign an email. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy and data security (using encryption).

You may generate public and private certificates for end users using Public Key Infrastructure (PKI) in on-premises environment. Public certificates are distributed to your on-premises Active Directory and stored in two attributes, which can then be replicated to your tenant in Office 365. Private certificates are distributed to end users and may be stored on their devices, smartcards, or other applications. You maintain control of the master key in your PKI infrastructure.

Further, Office 365 also provides capability for end users to compose, encrypt, decrypt, read, and digitally sign emails between two users in an organization using Outlook, Outlook Web App (OWA) or Exchange ActiveSync (EAS) clients.

An email that is encrypted using S/MIME can be decrypted only by the email recipient's private key. As such, an email message cannot be decrypted by anybody other than the recipient of the email if such an email is intercepted in transit or at rest.

You may find more information at http://technet.microsoft.com/library/dn626158.

Office 365 Message Encryption

Office 365 Message Encryption delivers confidential business communications with enhanced security, allowing users to send and receive encrypted email as easily as regular email directly from their desktops. Email can be encrypted without complex hardware and software to purchase, configure, or maintain, which helps to minimize capital investment, free up IT resources, and mitigate messaging risks.

Implementation of and protection of data with Office 365 Message Encryption thwarts the threats that may occur due to wire-tapping, man-in-the-middle attack, or various forms of digital interception. This is true for email messages sent internally and externally. At the same time, any unwarranted access of email messages (in transit or at rest) is prevented via policies intrinsic to the email messages themselves. This mitigates the risk of data falling in wrong hands either knowingly or unknowingly and provides further data loss prevention capabilities.

More information on OME can be found at http://technet.microsoft.com/library/dn569286.aspx. .

Anti-malware/anti-spam controls

You also have configuration options for anti-malware/anti-spam controls in the service. You may optionally choose to use your own anti-malware service and route to and from Office 365 via that third-party service. Office 365 uses multi-engine anti-malware

scanning to protect incoming, outgoing, and internal messages from malicious software transferred through email.

Your administrators can use the Office 365 Administration Center to manage anti-malware/anti-spam controls, including advanced junk mail options and organization-wide safe and blocked sender lists. Individual users can manage their safe and blocked senders from within their inboxes in Microsoft Outlook or Microsoft Outlook Web App.

Content controls and multi-engine malware scanning also help eliminate documents containing malicious code. Based on file name extensions, Office 365 blocks certain file types that can contain malicious code from being uploaded to or retrieved from the service. Office 365 uses an intelligent instant message filter (IIMF) to help protect the service and your networks against malware and spam via IM.

Transport Layer Security

You may setup an SMTP connection to their trusted partners that is secured using Transport Layer Security negotiation. The connector can be set to send emails using either opportunistic or forced TLS. More information can be found at http://technet.microsoft.com/en-us/library/exchange-online-mail-flow.aspx.

Sending email via an encrypted SMTP channel can prevent data in emails from being stolen in man-in-the-middle attack where one corporation is sending emails to their business partner.

Secure end-user access

Office 365 data and services are secured at the data center, network, logical, storage, and transit levels. In addition, it is critical to be able to control access to data and how it may be used. In the Office 365 service, Azure Active Directory is used as the underlying identity platform. This enables your tenant with strong authentication options granular control over how IT professionals and users can access and use the service. Office 365 also allows integration with an on-premises Active Directory or other directory stores and identity systems such as Active Directory Federation Services (ADFS) or third-party secure token systems (STSs) to enable secure, token-based authentication to services.

Federated identity and single sign-on security provisions

Your administrators can federate on-premises Active Directory or other directory stores with Azure Active Directory. After federation is configured, all Office 365 users whose identities are based on the federated domain can use their existing corporate logons to authenticate to Office 365. Federation enables secure, token-based authentication. This also allows administrators to create additional authentication mechanisms such as:

- Multi-factor authentication
- Client-based access control, allowing organizations to control how users access information from specific devices or specific locations or a combination of both (for example, limiting access from public computers or from public open Wi-Fi)

- Role-based access control (RBAC), similar to the access control procedure for Microsoft data centers described earlier in the "Automated operations" section

With IM federation, Lync Online users can IM in a highly secure environment with users in other organizations that use Lync Online, on-premises Lync Server 2010, and even the Skype public IM network. All federated communications are encrypted between the IM systems using access proxy servers. In addition, Lync Online allows administrators to save IM conversations.

Multi-factor authentication

Multi-factor authentication enhances security in a multi-device and cloud-centric world. We provide an in-house solution for multi-factor authentication with a phone call, text message, or notification on a dedicated app. We also support third-party multi-factor authentication solutions.

The Microsoft based multi-factor authentication options include:

- Call my mobile phone. The user receives a phone call that asks them to press the pound key. Once the pound key is pressed, the user is logged in.
- Text code to my mobile phone. The user receives a text message containing a six-digit code that they must enter into the portal.
- Call my office phone. This is the same as Call my mobile phone, but it enables the user to select a different phone if they do not have their mobile phone with them.
- Notify me through app. The user configured a smartphone app and they receive a notification in the app that they must confirm the login. Smartphone apps are available for Windows Phone, iPhone, and Android devices.
- Show one-time code in app. The same smartphone app is used. Instead of receiving a notification, the user starts the app and enters the six-digit code from the app into the portal.

Users who are enrolled for multi-factor authentication are required to configure App Passwords in order to use Office desktop applications, including Outlook, Lync, Word, Excel, PowerPoint, and OneDrive for Business.

Once your information worker has logged in with multi-factor authentication, they will be able to create one or more App Passwords for use in Office client applications. An App Password is a 16-character randomly generated password that can be used with an Office client application as a way of increasing security in lieu of the second authentication factor.

For more information about Multi-Factor Authentication for Office 365 please read the TechNet article Multi-Factor Authentication for Office 365

Privacy by Design

When you entrust your data to Office 365 you remain the sole owner: you retain the rights, title, and interest in the data you store in Office 365.

It is with this clarity of principle that we ensure that we maintain your privacy and operate our online services with certain key principles:

- We do not mine your data for advertising or for any other purpose other than providing you services that you have paid for.
- If you ever choose to leave the service, you take your data with you with full fidelity.
- We tell you where your data resides, who has access, and under what circumstances.
- Access to your data is strictly limited, non-destructive, logged and audited.[1]

Beyond this, we have privacy controls to allow you to configure exactly who has access to what within your organization. Strict controls and design elements prevent or mingling of your data with that of other organizations using Office 365 and from Office 365 data center staff having access to your data.

As a customer, you need to be able to trust that governments will respect your privacy as a citizen. Microsoft encourages government inquiry to be made directly to you unless legally prohibited and will challenge attempts to prohibit disclosure in court.

[1] *Sample third audits are performed to attest that access is only for appropriate business purposes*

Privacy Customer Controls

In addition to service-level capabilities, Office 365 enables you to collaborate through the use of transparent policies and strong tools while providing the distinct ability to control information sharing.

- **Rights Management in Office 365**—Allows individuals and administrators to specify access permissions to documents, workbooks, and presentations. This helps you prevent sensitive information from being printed, forwarded, or copied by unauthorized people by applying intelligent policies.
- **Privacy controls for sites, libraries and folders**—SharePoint Online, a key component service of Office 365 that provides collaboration functionality has a number of privacy controls. One example is that SharePoint Online sites are set to "private" by default. A second example is that a document uploaded to OneDrive for Business is not shared until the user provides explicit permissions and identifies who to share with.
- **Privacy controls for communications**—In Lync Online, another key component service that provides real-time communications in Office 365, there are various administrator-level controls as well as user-level controls to enable or block communication with external users and organizations. One example is blocking access to federation in Lync. Similarly there are controls throughout the service for the admins and users to ensure privacy of their content and communications.

Service Compliance

Operating a global cloud infrastructure creates a need to meet compliance obligations and to pass third-party audits. Auditable requirements come from government and industry mandates, internal policies, and industry best practices. Continuous compliance refers to our commitment to evolve the Office 365 controls and stay up to date with IT standards and regulations.

As a result, Office 365 has obtained independent verification, including ISO 27001 and SSAE16 SOC 1 (Type II) audits, is able to transfer data outside of the European Union through the U.S.-EU Safe Harbor Framework and the EU Model Clauses, is willing to sign a HIPAA Business Associate Agreement (BAA) with all customers, has received authority to operate from a U.S. federal agency under FISMA, and has disclosed security measures through the Cloud Security Alliance's public registry. Office 365 extends the controls implemented to meet these standards to customers who are not necessarily subject to the respective laws or controls.

ISO 27001

Office 365 service meets ISO 27001 standards and was the first major business productivity public cloud service to have implemented the rigorous set of global standards covering physical, logical, process, and management controls.

FISMA

Office 365 has been granted FISMA moderate Authority to Operate by multiple federal agencies. Operating under FISMA requires transparency and frequent security reporting to our U.S. Federal customers. Microsoft applies these specialized processes across our infrastructure to further enhance our Online Services Security and Compliance program for the benefit of customers who are not subject to FISMA requirements.

HIPAA BAA

Office 365 is the first major business productivity public cloud service provider to offer a HIPAA Business Associate Agreement (BAA) to all customers. HIPAA is a U.S. law that applies to healthcare entities—it governs the use, disclosure, and safeguarding of protected health information (PHI), and imposes requirements on covered entities to sign business associate agreements with their vendors that have access to PHI.

EU Model Clauses

Office 365 became the first major business productivity public cloud service provider to sign the standard contractual clauses created by the European Union (known as the "EU Model Clauses") with all customers. The EU Model Clauses address the international

transfer of data. Office 365 is one of very few cloud services—if not the only cloud service—that has received broad validation from European data protection authorities (DPAs) regarding its approach to the EU Model Clauses, including from Bavaria, Denmark, France, Ireland, Luxembourg, Malta, and Spain.

Further recently, Article 29 Working Party, a consortium of European data protection authorities, has publicly stated that our contractual commitments meet the requirements of the EU Model Clauses. Microsoft is the first cloud services provider to get such an approval from the Article 29 Working Party. You can read more about it in the blog here: http://blogs.office.com/2014/04/22/privacy-authorities-across-europe-approve-office-365-privacy-commitments/

Cloud Security Alliance

Office 365 meets compliance and risk management requirements as defined in the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM). The CCM is published by a not-for-profit, member-driven organization of leading industry practitioners focused on helping customers make the right decisions when moving to the cloud. The matrix provides a detailed understanding of the security and privacy concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. Office 365 has published a detailed overview of its capabilities for the CCM requirements that illustrates how these capabilities meet these requirements and empowers customers with in-depth information to evaluate different offerings in the marketplace today.

Customer Compliance Controls

With Office 365, we offer a range of compliance features, including data loss prevention (DLP), eDiscovery, and auditing and reporting functionality. Across these capabilities, the user experience is preserved and productivity is not impacted, leading to greater user acceptance.

Data loss prevention (DLP)

Although malware and targeted attacks can cause data breaches, user error is actually a much greater source of data risk for most organizations. Exchange Online provides data loss prevention (DLP) technology that identifies, monitors, and protects sensitive data and helps users understand and manage data risk. For example, DLP proactively identifies sensitive information in an email message, such as social security or credit card numbers, and alerts users via "Policy Tips" before they send that message. Your administrators have a full range of controls and can customize the level of restrictions for their organization. For example, users can simply be warned about sensitive data before sending—sending sensitive data can require authorization, or users can be blocked from sending data completely. DLP features scan both email messages and attachments, and your administrators have access to comprehensive reporting about what data is being sent by whom. Administrators can also apply RMS for content that is triggered by a DLP rule.

Additionally, you may encounter scenarios in which individuals in your organization handle many kinds of sensitive information during a typical day. Document Fingerprinting makes it easier for you to protect this information by identifying standard forms that are used throughout your organization.

This data loss prevention capability is being expanded to other aspects of the service like SharePoint Online in the near future.

Auditing and retention policies

By using Office 365 auditing policies, your users can log events, including viewing, editing, and deleting content such as email messages, documents, task lists, issues lists, discussion groups, and calendars. When auditing is enabled as part of an information management policy, administrators can view the audit data and summarize current usage. Administrators can use these reports to determine how information is being used within the organization, manage compliance, and investigate areas of concern.

For business, legal, or regulatory reasons, you may have to retain e-mail messages sent to and from users in your organization, or you may want to remove e-mail that you aren't required to retain. Messaging records management (MRM), the records

management technology in Office 365, enables you to control how long to keep items in users' mailboxes and define what action to take on items that have reached a certain age.

MRM in Office 365 is accomplished by using *ion tags* and *retention policies*. An overall MRM strategy is based on:

- Assigning *retention policy tags* to default folders, such as the Inbox and Deleted Items.
- Applying *default policy tags* to mailboxes to manage the retention of all untagged items.
- Allowing the user to assign *personal tags* to custom folders and individual items.

Separating MRM functionality from users' Inbox management and filing habits. Users aren't required to file messages in managed folders based on retention requirements. Individual messages can have a different retention tag than the one applied to the folder in which they're located.

eDiscovery

The new, easy-to-use eDiscovery Center can be delegated to your specialist users—such as a compliance officer or human resources personnel—to conduct eDiscovery tasks without having to generate additional overhead for the IT department. Using eDiscovery, compliance officers can retrieve content from across Exchange Online, SharePoint Online, and Lync Online. With the integrated Office 365 eDiscovery, you have one single experience for searching and preserving email, documents, and site mailboxes. You can be specific about what to search for and preserve. The ability to find only what you want and nothing more can contribute to a reduction of discovery costs. The eDiscovery process places no burden on the user for preserving and searching for data, because all of these processes are performed in the background.

Data spillage management

Office 365 has compliance features to support you if your organization ever needs to manage data "spillage." For example, if a federal government organization were to transmit classified data into Office 365, there are ways for the organization to remove the data by themselves. Compliance and security officials with appropriate RBAC privileges can use eDiscovery to search for the message or document and hard-delete them. The hard drives used to store the "spilled" data are never re-purposed or repaired or otherwise moved out of the physical security of the Office 365 data center. They are destroyed if they are no longer used in the Office 365 infrastructure.

Data deletion

Customer data privacy is one of our key commitments for the cloud. With Office 365, at contract termination or expiration, we will provide at least 90 days for your administrators to confirm all data migration have been completed, at which point the data will be destroyed to make it unrecoverable. Further, we provide guidelines to your administrators to personally destroy data if that is preferred. Electronic discovery can be performed to verify that no data can be returned.

Conclusion

Businesses today need productivity services that help users get more done from virtually anywhere while maintaining security in the face of ever-evolving threats. Office 365 supports both of these needs at once with a highly secure, cloud-based productivity platform. Information regarding Office 365 security, privacy, compliance, transparency, and service continuity can be found in the Office 365 Trust Center. The Office 365 platform incorporates security at every level, from application development to physical data centers to end-user access. Today, fewer and fewer organizations have the ability to maintain an equivalent level of security on-premises at a reasonable cost.

Importantly, Office 365 applications include both built-in security features that simplify the process of protecting data and the flexibility for administrators to configure, manage, and integrate security in ways that make sense for their unique business needs. When businesses choose Office 365, they get a partner that truly understands business security needs and is trusted by companies of all sizes across nearly every industry and geography.