OneDrive for Business

SharePoint

# File security in Microsoft SharePoint and OneDrive for Business

Microsoft

*Published September 2016*
*Revised October 2016*

# Contents

## Protecting your files in SharePoint and OneDrive for Business

When choosing a cloud collaboration platform, the most important consideration is trust in your provider. Microsoft SharePoint and OneDrive for Business are covered by the core tenets of earning and maintaining trust: security, privacy, compliance, and transparency. With SharePoint and OneDrive, they're your files. You own them and control them.

The Microsoft approach to securing your files involves:

1. A set of customer-managed tools that adapt to your organization and its security needs.
2. A Microsoft-built security control framework of technologies, operational procedures, and policies that meet the latest global standards and can quickly adapt to security trends and industry-specific needs.

These tools and processes apply to all Microsoft Office 365 services—including SharePoint and OneDrive—so all your content beyond files is secure.


Microsoft focuses its investments in the following areas:

1. Platform security
    a. Infrastructure and processes of our datacenters
    b. Strong encryption technologies (at rest and in transit)
2. Secure access and sharing
    a. Restrict access to files to approved people, devices, apps, locations, and data classifications
    b. Enforce who can share files and with whom
3. Awareness and insights
    a. Complete understanding of how people in your organization are using SharePoint and OneDrive
    b. Analyze usage to measure return on investment
    c. Identify potentially suspicious activity

4. Information governance
    a. Classify what constitutes sensitive data and enforce how it can be used
    b. Protect your organization in the event of litigation
    c. Retain business-critical files when people leave your organization
5. Compliance and trust
    a. Ensure that service operations are secure, compliant, trustworthy, and transparent

Microsoft delivers a comprehensive, flexible security framework that adapts to IT needs but delivers user-friendly experiences. SharePoint and OneDrive offer simple and powerful ways to work with files on any device, as well as seamless integration with leading productivity tools such as Office. User simplicity is balanced with the need for your organization to protect important business files.

Let's look at how you can manage the right security plan for your organization and how Microsoft provides support.

## *Platform security*


Platform security is one of the most important design principles and features of Office 365. It spans hardware, software, datacenter premises security, independent audit verification, and operational policies.

### Physical security

Platform security starts with protecting Microsoft datacenters, which are built from the ground up to protect services and data from harm by natural disaster or unauthorized access. Access to our

datacenter facilities is restricted by job function, with only customer application and services access given to essential personnel. Datacenters are guarded by inner and outer perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, multi-factor access control, integrated alarm systems, and extensive 24/7 video surveillance from the operations center. Datacenters are globally distributed while taking into account regional data location considerations.

Network security only allows connections and communications that are necessary for systems to operate. Networks within datacenters provide physical separation of critical back-end servers and storage devices from public-facing interfaces. The location of specific customer data is unintelligible to the personnel that have physical access to our datacenters. Faulty hardware, including drives, is demagnetized and destroyed when decommissioned.

### Logical security

Most of the operations performed by our administrators are automated so that human intervention is reduced to a minimum, decreasing the possibility of an inconsistent configuration or malicious activity. System deployment is also automated in our datacenters. Administrator access to your files is strictly controlled. A combination of port scanning, perimeter vulnerability scanning, and intrusion detection prevents malicious access.

### Customer Lockbox

Microsoft personnel do not have standing access to your data. In the very rare event that a support engineer needs to access your data to resolve an issue at your request, Customer Lockbox extends access control to you so you grant final approval for access.

### Vigilance

Microsoft regularly monitors production environments for privacy and security-related threats. Microsoft uses a thorough internal program that reports potential privacy risks in datacenters. When activated, engineers work together with specialists with a background in privacy, forensics, legal, and communications to determine the appropriate course of action to ensure that any incidents are resolved quickly.


### Encryption in transit and at rest

File security starts with encryption in transit and at rest in Microsoft datacenters. Your files are safeguarded with some of the strongest encryption and detection technologies available. That's our duty as your cloud storage provider. Every file in SharePoint and OneDrive is encrypted in transit (TLS 1.0, 1.1, and 1.2) between the user's browser, PC, Mac, or mobile device and our datacenters. All connections are established using 2048-bit keys.

Once the file reaches the Microsoft datacenter, the files are encrypted through two components: BitLocker disk-level encryption and per-file encryption. BitLocker encrypts all data on a disk. Per-file encryption goes even further by including a unique encryption key for each file. Furthermore, every update to every file is encrypted using its own encryption key. Before they're stored, the keys to the encrypted files are themselves encrypted and stored in a physically separate location.

Every step of this encryption uses Advanced Encryption Standard (AES) with 256-bit keys and is Federal Information Processing Standard (FIPS) 140-2 compliant. The encrypted content is distributed across several containers throughout the datacenter, and each container has unique credentials. For details on these features, see our guide to Service Assurance in the Security and Compliance Center.

### Customer-controlled encryption keys

Coming soon, you'll have the option to encrypt content at rest with customer-controlled encryption keys for files stored in SharePoint Online and OneDrive for Business. Sometimes referred to as "bring your own key," customer-controlled encryption keys enable you to store and manage your own encryption keys, which may help you meet certain compliance obligations. If you choose to use customer-controlled encryption keys, you control the root keys that Office 365 services will use to encrypt and decrypt your data, as well as the permissions to use those keys.

You can also use customer-controlled keys to leave Office 365 and render all customer data stored in Office 365 unreadable by Office 365 services. This is accomplished by removing access to the encryption keys used to encrypt the data.

### Other encryption options

In addition to the encryption provided by Office 365, Microsoft Azure Rights Management (Azure RMS) uses encryption, identity, and authorization policies to further secure your files and email. Azure RMS works across phones, tablets, and PCs and helps protect the small percentage of ultra-sensitive data that is mission-critical for your organization. Information can be protected both within and outside your organization because the protection remains with the data, even when it leaves your organization's boundaries.

## *Awareness and insights*

Having clear visibility into everything that is going on with your files is important for two key reasons:

1. Measuring the usage of the system is a vital metric in determining your return on investment (ROI).
2. Visibility into user actions enables you to ensure compliance with governance guidelines, identify potential misuse, and develop appropriate policies informed by usage patterns.

### Auditing and alerting

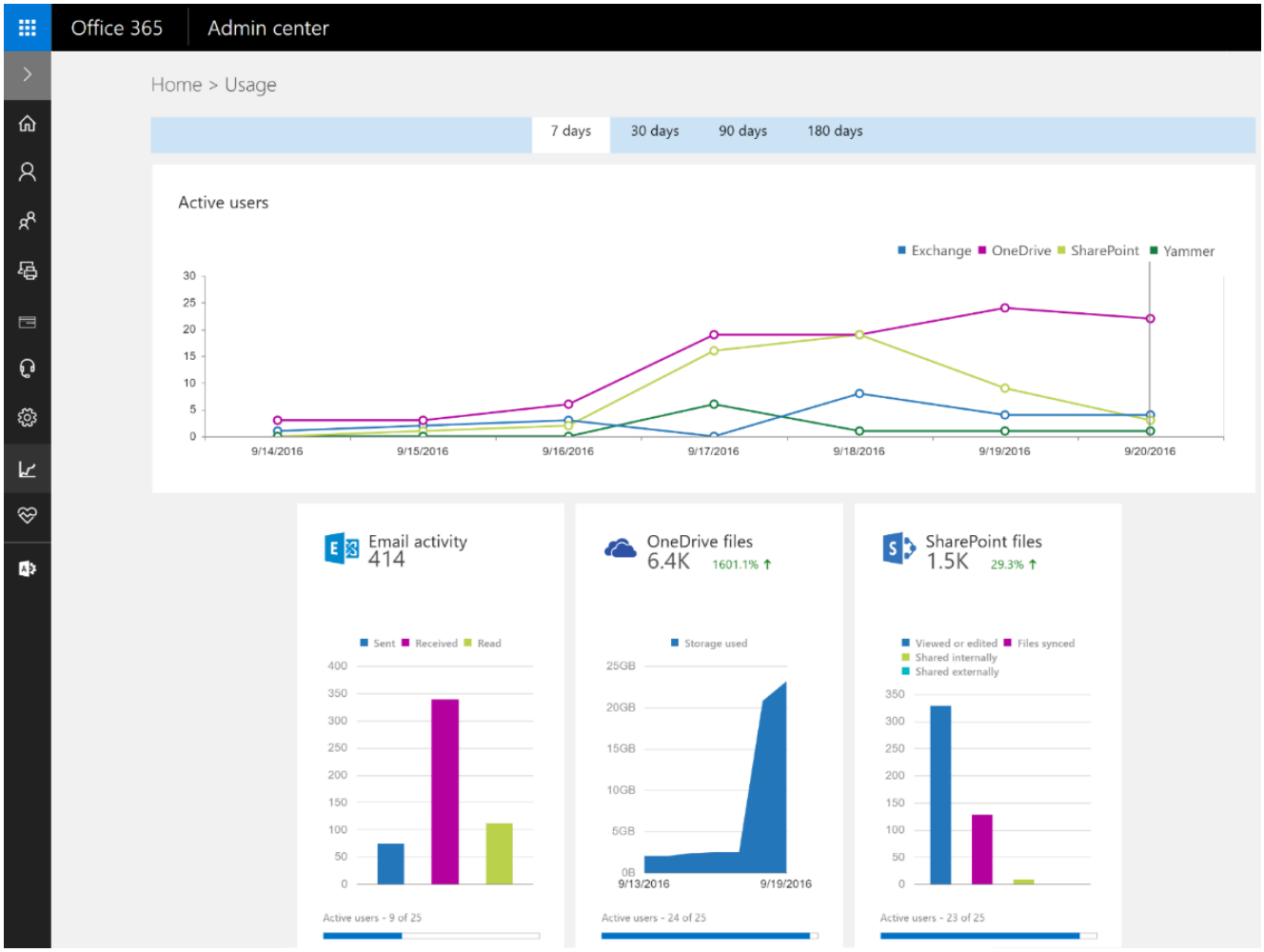
Every user and administrative action on SharePoint and OneDrive is recorded for a full audit trail. This includes key file operations like tracking every time a user accesses, modifies, downloads, shares, or uploads a file. Administrators can filter this data by date, time, user, file, IP address, and action. This filtered view can be exported to a CSV file if required. Administrators can also set up custom alerts so that whenever a specific event occurs, an action such as an email notification can be triggered.

For organizations moving to SharePoint and OneDrive, Microsoft is introducing unified auditing across SharePoint Online and on-premises SharePoint. Unified auditing provides one seamless way to review activity across all your files. For organizations and developers who want to do more, all audit data is

provided through the [Office 365 Management Activity API](#).

### Reporting

The Office 365 admin center provides a full usage dashboard that makes it easy to monitor all Office 365 services and identify issues and opportunities, such as the need for user awareness or training. Included in the dashboard is an active user count, file storage utilized, and a drill-down into each user to see last activity date, number of files, and storage used.




## *Secure access and sharing*

Access controls have traditionally been scoped to users or groups. Today, a user's work is no longer limited to one computer on a desk, and information risks exposure as users connect mobile devices to unsecure networks or use personal, unmanaged devices.

Conditional access in SharePoint and OneDrive goes beyond user permissions. It is based on a combination of factors, such as:

- The identity of a user or group
- The network that the user is connected to
- The device and application they are using
- The type of data they are trying to access

The access granted to the user adapts to this broader set of dynamic conditions. Using SharePoint and OneDrive, you can ensure that only the right people can access the right data under the right circumstances.

Beyond conditional access, SharePoint and OneDrive also provide precise controls over who can share files and with whom to prevent oversharing.

### Conditional access

*Managing users and groups*

Ensure that the right people have access to the right data. Office 365 includes the industry leading enterprise identity management service: Microsoft Azure Active Directory (AAD). With AAD, your administrators can manage users and groups, enforce strong passwords, set up multi-factor authentication, and enable conditional access. In addition, AAD can federate with on-premises Active Directory or other directory stores so users can authenticate to Office 365 with their existing corporate logons.

*Device management*

In a world where the expectation is that data is available from anywhere, you want to ensure your data is safe across all devices—both managed and unmanaged. Users are increasingly mobile and use multiple devices, including personal devices, to access organizational data. It is important to enable users to be productive on any device while maintaining the security of data across all devices. Device access policies in Office 365 allow you to decide the level of access you want to offer based on the management state of each device.

Microsoft Enterprise Mobility + Security (EMS) allows you to customize the definition of a managed device to fit the needs of your organization. You can either grant full access, prevent all access, or allow restricted access from unmanaged devices. EMS can define a frontier of managed devices while

still permitting appropriate productivity on unmanaged devices (sometimes called "bring your own device," or BYOD). The restricted access policy allows a user to view a file in their browser but does not allow them to download, print, or sync. This allows users to be productive on personal, unmanaged devices, but at the same time, prevents accidental leakage of data to devices that are not managed by your organization.

When setting any of these policies, you also default to blocking access from any apps that can't enforce device-based restrictions.

*Application management*

Using Microsoft Intune Mobile Application Management (MAM), you can control which apps have access to files on both SharePoint and OneDrive and prevent corporate data leaks by restricting actions in Office mobile apps such as Cut, Copy, Paste, and Save As. The Intune MAM solution integrates seamlessly with Microsoft Mobile Device Management (MDM) capabilities, but can also be deployed alongside other Enterprise Mobility Management (EMM) solutions.

Coming soon, SharePoint and OneDrive will deliver a single admin experience that allows you to simply set Microsoft Intune policies without having to go to a different admin console.

*Location-based access*

With location-based conditional access policies in SharePoint and OneDrive, you can limit access to specific corporate networks or locations. For example, if you restrict access to only your corporate network, users will not be able to access organizational data when they leave the office. This policy helps prevent access to your organization's data from rogue or insecure networks. It can also ensure that all traffic in the organization comes through virtual private networks (VPNs) and transits to public edgepoints through known, managed infrastructure.

### Secure sharing

Sharing is a core scenario for SharePoint and OneDrive. IT and end users should have confidence that the files they share are accessed by the right people under the right conditions.

Users receive visual prompts and tips about the number of people that will have access to a file or folder when they're sharing it.  They're also alerted when sharing content outside your organization—helping avoid mistakes that occur when they're unaware of content visibility.

There are a range of controls for administrators to govern who can share files (internally, externally, or both) and who they can be shared with. Examples include:

- Restricting which files can be shared with external users
- Turning off external sharing permissions for specific sites and users

- Restricting sensitive content from being shared externally
- Blocking sensitive files from being attached to emails
- Governing the duration that external share links are accessible
- Configuring an allow list and a deny list of external domains for sharing

## *Information governance*

Office 365 provides a comprehensive set of governance tools that apply to files in SharePoint and OneDrive. These tools allow you to define what sensitive data is and what happens if this sensitive data is saved to SharePoint or OneDrive.

If a user leaves or is terminated from your organization, flexible data retention policies give you confidence that data loss won't occur.

Finally, you may need to respond to information requests due to internal investigations, regulatory requests, litigation, or other administrative inquiries. Manually finding and organizing content for these requests is a huge burden for most organizations around the world. With our suite of eDiscovery solutions, you can find the relevant content, place it under legal hold, and use machine learning to improve the accuracy and relevance of eDiscovery results.

### Sensitive data protection policies

Although security issues like malware and targeted attacks are concerns, user error is a much greater source of data risk for most organizations. SharePoint and OneDrive provide 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 data in files, such as social security numbers, and alerts users via Policy Tips. Administrators have a full range of configurable controls for their organization. Users can simply be warned about sensitive data, or users can be blocked from finding, opening, or sharing files completely.

### Data retention

Data retention policies allow companies to comply with their own organizational or industry compliance requirements. Administrators can choose to set global retention policies on all content, granular policies on specific users, or content based on tags, last modified date, or created date. With data retention, you can both preserve and delete content from across all Office 365 services on your own schedule.

### eDiscovery

eDiscovery and legal hold capabilities help you find, preserve, analyze, and package electronic content

(often referred to as electronically stored information or ESI) in the event of an internal investigation, regulatory request, or legal request. Control of eDiscovery can be delegated to specialists such as compliance officers or human resources personnel, eliminating unnecessary overhead for your IT department. Using eDiscovery, content across Microsoft Exchange, OneDrive, SharePoint and Skype for Business can easily be retrieved and preserved. You can specify what to search for and preserve with no end-user action required, as these processes are performed in the background.

Office 365 Advanced eDiscovery integrates machine learning, predictive coding, and text analytics capabilities to reduce the costs and challenges that come along with sorting through large quantities of data for eDiscovery purposes. In today's high-volume data environment, the eDiscovery process for any given case could involve sorting through thousands of emails, text messages, instant messages, and documents to find the small number of files that are most likely to be relevant. Office 365 Advanced eDiscovery reduces the volume of data by eliminating duplicate files, reconstructing email threads, and identifying key themes and data relationships. Finally, it enables predictive coding, allowing users to train the system to intelligently explore and analyze large, unstructured data sets and quickly zero in on what is likely to be relevant.

## *Compliance and trust*

You need a ready-to-go productivity solution that is secure and trustworthy, and allows you to meet your organizational, statutory, and industry compliance needs.

### Proactive compliance

Office 365 is a global service, and continuous compliance refers to our commitment to evolve the Office 365 controls to stay up to date with standards and regulations that apply to your industry and region. A team of compliance specialists continuously tracks standards and regulations, developing common control sets for our product team to build into the service. Over 900 controls are built into the Office 365 compliance framework that enable Office 365 to stay current with ever-evolving industry standards. To help organizations comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data, Microsoft offers the most comprehensive set of certifications and attestations of any cloud service provider. As key components of Office 365, SharePoint and OneDrive benefit from this focus on continuous 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. Office 365 has obtained broad independent verification, including:

| | |
|---|---|
| **ISO 27001** | Office 365 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. |
| **ISO 27018** | Microsoft was the first major cloud service provider to be independently verified as meeting ISO 27018. |
| **SSAE 16** | Office 365 has been audited by independent third parties and can provide Statement on Standards for Attestation Engagements No. 16 (SSAE 16) SOC 1 Type I and Type II and SOC 2 Type II. |
| **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 was the first major business productivity public cloud service provider to offer a HIPAA Business Associate Agreement (BAA) to all customers. |

| | |
|---|---|
| **EU Model Clauses** | Office 365 was 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 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, the 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. |
| **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. |

### Privacy

When you entrust your files to SharePoint and OneDrive, you remain the sole owner of those files: you retain the rights, title, and interest. You know where your files reside, who has access, and under what circumstances. It's Microsoft policy to only use your content for purposes consistent with providing you cloud productivity services, and not mine it for advertising purposes. If you ever choose to leave the service, you can take your files with you with full fidelity. Customer data privacy is one of the key commitments for the cloud in Office 365.

With Office 365, at contract termination or expiration, you are provided at least 90 days for your administrators to confirm all data migration has been completed, after which your content will be destroyed to make it commercially unrecoverable. Microsoft regularly discloses the number of law enforcement requests received through transparency reports. If approached by a government for access to customer data, Microsoft redirects the inquiry to you, the customer, whenever possible. Microsoft has challenged and will challenge in court any invalid legal demand that prohibits disclosure of a government request for customer data. Finally, SharePoint sites and libraries are set to "private" by default and files uploaded to OneDrive are not shared until the user explicitly takes a sharing action.

### Transparency

Moving to a cloud service shouldn't mean losing the ability to know what's going on. With SharePoint and OneDrive, it doesn't. We are transparent in our operations so you can monitor the state of your service, track issues, and have a historical view of availability. Office 365 maintains multiple copies of your data, across datacenters, for redundancy, and shares with you where your data is located and will provide one-month notice if the region where your data is stored is expanded into a new country. You can easily find who has access to your data and under what circumstances. You have 24/7 phone support for critical issues. Office 365 has DevOps processes, which means 24/7 escalation to the actual development team to resolve issues that cannot be resolved by operations alone. In the event of a service incident, Microsoft conducts a thorough review, regardless of the magnitude of the impact, and shares the analysis if your organization has been affected. Office 365 commits to delivering at

least 99.9% uptime with a financially backed guarantee.

## Summary

Microsoft approaches security for your files relentlessly, balancing it with a simple and powerful collaboration experience. We offer industry leadership in cloud operations, global scale, security, and compliance. Security of files is not an add-on. It is core to everything we do in SharePoint and OneDrive and extends to every service in the Office 365 suite. When businesses choose Microsoft, they get a partner that truly understands business security needs and is trusted by companies of all sizes across nearly every industry and geography.

For the latest information on Office 365 security and compliance, visit the Office 365 Trust Center.