Security and Service Continuity for Enterprises

Service Description

Published: June 28, 2011

For the latest information, please see Microsoft Office 365.

.

Contents

Introduction

Microsoft® Office 365 delivers the power of cloud productivity to businesses of all sizes, helping to save time and money and free up valued resources. Office 365 combines the familiar Office desktop suite with cloud-based versions of our next-generation communications and collaboration services: Microsoft Exchange Online, Microsoft SharePoint® Online and Microsoft Lync Online.

Companies can benefit from cloud services like Office 365. Microsoft knows that when allowing an external service provider to store and manage their data, companies consider security, data protection, privacy, and data ownership. Microsoft takes these concerns seriously and has applied its years of cloud and on-premises experience with security and privacy to the Office 365 services.

This service description describes the security, continuity, privacy, and compliance policies and controls for the Office 365 for enterprises service offerings. It is intended to provide Office 365 customers with an overview of how each of the Office 365 services is designed to provide a high degree of **security, privacy, continuity,** and **compliance** service goals that are derived from the Microsoft Risk Management program.

Microsoft Office 365 Security

The security architecture of Microsoft Office 365 has been designed using key principles of the Microsoft Trustworthy Computing initiative. To ensure that customer data is highly safeguarded from risks and threats, Microsoft applies a common set of security policies to the Office 365 services through the Microsoft security program. Office 365 services operate in compliance with these security policies and relevant industry standards. Microsoft is committed to continually improving and evolving Office 365 services to ensure customers are highly protected from current and future threats.

This section describes how Microsoft protects customers' business data and delivers Office 365 services securely and reliably. It also describes how Microsoft enhances security for each of the Office 365 services.

Note

For more information about industry-standard certifications and compliance certifications, see the Microsoft Office 365 Compliance section.

Securing Office 365 Services

Microsoft helps comprehensively secure Office 365 services by applying the Microsoft Security Management approach, which ensures that the security of Office 365 services is vigilantly maintained, regularly enhanced, and routinely verified through testing. This approach provides protection at multiple levels, including:

- **Physical layers at data centers:** Physical controls, video surveillance, access control
- **Logical layers:** Data isolation, hosted applications security, infrastructure services, network level, identity and access management, federated identity and single sign on.

Physical Security

Microsoft ensures that the environment in which the Office 365 customer's data is stored is physically secured by controlling accessibility through multiple security checks. These physical security checks are applied at multiple levels in the Microsoft data centers, and Office 365 services are delivered through carrier-class data centers that ensure consistent delivery according to the services' service-level agreements (SLAs). These data centers include the following industry-standard features:

- Secure physical access for authorized personnel only: Access is restricted by job function so that only essential personnel receive authorization to manage customers' applications and services. Physical access authorization utilizes multiple authentication and security processes: badge and smartcard, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication for physical access to the data center environment.
- Redundant power supplies, including two separate power feeds into each data center, battery backup, and diesel generators (with alternative fuel delivery contracts in place).
- Climate control to ensure that equipment runs at optimal temperature and humidity.
- Natural disaster control, including seismically braced racks where required and fire prevention and extinguishing systems.
- Physical monitoring, including motion sensors, 24-hour secured access, video camera surveillance, and security breach alarms.

- Worldwide Microsoft data center locations: Office 365 services are deployed in Microsoft data centers that are located around the world, and offer geographically local hosting with global availability.
- Secure network design and operations: The networks within the Office 365 data centers are designed to create multiple separate network segments within each data center. This segmentation helps to provide physical separation of critical, back-end servers and storage devices from the public-facing interfaces.
- Exceptional hardware: The underlying hardware used in Microsoft data centers is specifically designed to operate as efficiently, effectively, and securely as possible. The hardware helps Microsoft eliminate unnecessary costs, save power and space consumption, and pass on these savings to Office 365 customers.

Logical Security

Logical security in Office 365 is just as important as physical security. The following key features provide logical security for the delivery of Office 365 services:

- **Data isolation:** Data storage and processing is logically segregated among customers of the same service through Active Directory® structure and capabilities specifically developed to help build, manage, and secure multitenant environments. The multitenant security architecture ensures that customer data stored in shared Office 365 data centers is not accessible by or compromised to any other organization. Organizational units (OUs) in Active Directory control the prevention of unauthorized and unintended information transfer via shared system resources. Tenants are isolated from one another based on security boundaries, or silos, enforced logically through Active Directory.
- **Hosted applications security:** Microsoft ensures that applications hosted by Microsoft data centers are highly protected by robust security features and security measures that control access. These features include:
  - Support for authenticated and encrypted communications that help identify messaging participants and prevent message tampering.
  - Support for Secure/Multipurpose Internet Mail Extensions (S/MIME) encryption technologies in email messages.
  - Restricted message relaying to reduce unwanted messaging and spam.
  - Real-time block lists (RBL) and safe lists to restrict messages from known sources of spam.
  - Flexible device policies to help secure communications from mobile devices (such as PIN lock and remote or local wipe).
  - Protection against malicious software (also called malware) by implementing multilayered antivirus software for server operating systems, email messaging systems, and shared data.
  - Active Directory Rights Management Services, which helps users secure data that is stored at rest in Microsoft data centers. Active Directory Rights Management Services encrypts data and controls rights and permissions to that data stored in email or on SharePoint.

Note
Active Directory Rights Management Services is not offered by Microsoft as part of Office 365 services. Office 365 customers can purchase Active Directory Rights Management Services separately from Microsoft and deploy it in their data centers.

- **Security Development Lifecycle:** Microsoft applies Security Development Lifecycle, a software security assurance process, to design, develop, and implement Office 365 services. Security Development Lifecycle helps to ensure that communication and collaboration services are highly secured even at the foundation level. Through controls like Establish Design Requirements, Analyze Attack Surface, and Threat Modeling, Security Development Lifecycle helps Microsoft identify:

  - Potential threats while running a service.
  - Exposed aspects of the service that are open to attack.

  If potential threats are identified at Design, Development, or Implementation phases, Microsoft can minimize the probability of attacks by restricting services or eliminating unnecessary functions. After eliminating the unnecessary functions, Microsoft reduces these potential threats in the Verification phase by fully testing the controls in the Design phase.

- **Secured Office 365 services infrastructure:** Infrastructure-level security measures include:

  - User interfaces with security settings can be filtered by group permissions, which display available features to only the actions, links, and content that users are authorized to access.
  - Extensive server monitoring support integrated with the overall Microsoft System Center Operations Manager monitoring architecture.
  - Secure remote access via Microsoft Windows Server® 2008 Remote Desktop Services.
  - Multi-tier administration, using a three-tier administration model that isolates administrative tasks and controls access based on user role and the level of authorized administrative access.
  - Environmental security scanning to monitor for vulnerabilities and incorrect configuration.
  - Intrusion detection systems to provide continuous monitoring of all access to the Office 365 services. Sophisticated correlation engines analyze this data to immediately alert staff of any connection attempts that are classified as suspicious.
  - Security standards for operating systems to help protect Office 365 services from attack by malicious users or malicious code, including disabling nonessential services, securing file shares to require authorization, and implementing the Data Execution Prevention (DEP) feature. DEP is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running.
  - Systems management and access control using Active Directory. Active Directory manages networks and component servers that run the Office 365 services. Applications that provide the online services are designed to operate efficiently and effectively within the Active Directory environment.
  - Central management of security policies. The Microsoft staff manages and enforces security policies centrally from secured servers that are dedicated to controlling and monitoring network-wide systems. A delegated management model enables administrators to have only the access they need to perform specific tasks, reducing the potential for error and allowing access to systems and functions strictly on an as-needed basis.
  - New servers can be quickly and safely configured, and template-based server hardening ensures that new capacity is brought online with security measures already in place.

- **Network-level security measures:** These measures include features related to providing a highly secured connection over the Internet:

  - Customer access to services provided over the Internet originates from users Internet-enabled locations and ends at a Microsoft data center. These connections established between customers and Microsoft data centers are encrypted using industry-standard Transport Layer Security (TLS) /Secure Sockets Layer (SSL). The use of TLS/SSL effectively

establishes a highly secure browser-to-server connection to help provide data confidentiality and integrity between the desktop and the data center.
- A redundant network provides full failover capability and helps ensure 99.9-percent network availability.
- All remote connections by Microsoft operations personnel must be made via Remote Desktop Services.

- **Identity and access management:** Access to the systems hosting Office 365 services is controlled through the following methods:
  - Staff-level access control: Data center staff's access to the IT systems that store customer data is strictly controlled.

Access control follows the separation of duties principle and granting least privilege.

- Proactive host security: SharePoint Online security is enhanced by proactively securing the host system.
  - Server hardening by disabling unnecessary services
  - Logging and auditing
- Restricted access to services:
  - Content inspection
  - Hardened servers
  - Sessions better protected by SSL/TLS

> **Note**
>
> Access from mobile devices depends on wireless capability or mobile network availability.

- **Federated identity and single sign on:** With on-premises Active Directory, administrators can use single sign on for Office 365 services authentication. To achieve this, administrators can configure on-premises Active Directory Federation Services, a Windows Server 2008 service, to federate with the Office 365 services federation gateway. After Active Directory Federation Services is configured, all Office 365 users whose identities are based on the federated domain can use their existing corporate logon to automatically authenticate to Office 365.

Delivering Reliable Services

To ensure the reliability of Office 365 services, Microsoft focuses on effective deployment, administration, and maintenance.

- **Operations management and service deployment:** Operations is a key component of Office 365 services and is central to overall security and availability of these services. Operations management practices for Office 365 (for example, change management, incident and problem management) are based upon industry-standard principles of the Information Technology Infrastructure Library (ITIL). Microsoft has added the Microsoft Operations Framework (MOF), a standardized implementation of ITIL recommendations, which provides an integrated set of best practices, principles, and activities that help organizations achieve reliability for their IT solutions and services.

Office 365 maintains a dedicated security organization that is focused on constant security vigilance, with a staff that follows the principles defined in MOF. The security team adheres to the following functions defined by ITIL and applies them to the operation of the Office 365 services:

- Change management
- Incident management
- Problem management

In addition, the Office 365 services require distinct hosted services development, deployment, and operations staff to adhere to the principle of segregation of duty. This includes controlling access to the source code, build servers, and production environment. For example:

- Access to the Office 365 services production environment is restricted to operations personnel. Development and test teams may be granted temporary access to help troubleshoot issues.
- Access to the Office 365 services source code control is restricted to development personnel; operations personnel cannot change source code.

- **Monitoring and risk reduction:** Microsoft makes significant investments in developing tools and services for monitoring Office 365 and its environment.

  - Microsoft System Center Operations Manager: Servers within the Office 365 services environment are configured to maximize the reporting of security events from the operating system and applications. The Office 365 services operations team uses the latest technology and optimized processes to harvest, correlate, and analyze information as it is received. System Center Operations Manager is an end-to-end service management environment that integrates with platform and services hardware and software to provide continuous health monitoring. System Center Operations Manager management packs provide internal transaction monitoring, capabilities for looking at service threshold models, and CPU utilization analysis that is tailored to the Office 365 service applications. In addition, custom management packs are layered above the Office 365 platform to provide operations staff with very specific information that helps identify trends and predict behavior that may require proactive intervention.
  - Integrated infrastructure and web performance monitoring**:** System Center Operations Manager data is combined with feeds from additional specialized tools and services to capture, aggregate, and analyze the network that operates Office 365 services as well as the behavior of key sites on the Internet. For example, if connectivity begins to degrade, staff can identify whether the problem is internal to one of the Office 365 services or caused by conditions on the Internet that may represent a risk to Office 365 customers.
  - Hardware and software subsystems monitoring: Proactive monitoring continuously measures the performance of key subsystems of the Office 365 services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event. The following list describes some specific thresholds:

    - CPU utilization: When utilization reaches 80 percent, a non-critical alert is displayed. When utilization reaches 90 percent, a critical alert threshold is displayed.
    - Service utilization: Various service components, including service licenses; capacity for email; and Microsoft SharePoint Online, are all monitored.
    - Storage utilization: If storage reserves are reduced to 15 percent, a non-critical alert is displayed. If storage reserves reach 7 percent, a critical alert is displayed.

- Network latency: When network latency is at 100 milliseconds, a non-critical alert is displayed. When network latency is at 300 milliseconds, a critical alert is displayed.

Exchange Online Security

In addition to securing the overall environment from which the Office 365 services are delivered, Microsoft ensures that security elements are also included in the individual Office 365 services.

The Exchange Online service is enabled through Exchange Server 2010, which offers a wide range of security features, including:

- **Anti-spam and antivirus filtering:** Exchange Online uses Microsoft Forefront® Online Protection for Exchange an email filtering technology to help protect incoming, outgoing, and internal messages from malicious software transferred through email. It ensures that all messages transported through Exchange Online service are scanned for viruses and malicious software.

  This service uses proprietary anti-spam technology to help achieve high accuracy rates of blocking spam messages from reaching the corporate network. Forefront Online Protection for Exchange uses multiple complementary antivirus engines to help detect viruses and other malicious code spread through email.

  Exchange Online also supports features for Safe and Blocked Senders, Junk Mail and Spam Quarantine, and Filtering Service for Inbound Email. For more information on these features, see the Exchange Online Service Description.

- **Custom routing of outbound email:** Exchange Online provides the ability to route outbound mail through an on-premises server or a hosted service (sometimes called smart hosting). This capability allows organizations to use data loss prevention (DLP) appliances, perform custom post-processing of outbound email, and deliver email to business partners via private networks.
- **Transport layer security (TLS):** The TLS encryption mechanism encrypts the connection between Exchange Online servers and client to help prevent spoofing and provide confidentiality for email messages in transit. TLS is also used for securing customers on-premises mail server traffic to Exchange Online during migration and coexistence scenarios.

  Exchange Online supports opportunistic TLS as well as forced TLS. For more information, see the Exchange Online Service Description.

- **Encryption between clients and Exchange Online:** Client connections to Exchange Online use the SSL to enhance security:
  - Securing Microsoft Outlook®, Outlook Web App, Exchange ActiveSync®, and Exchange Web Services traffic using TCP port 443.
  - Securing POP3 and IMAP using TCP port 995.
- **S/MIME:** Exchange Online will transport and store S/MIME messages.

Note

Exchange Online does not host S/MIME functions and does not provide key repository, key management, or key directory services.

- To use S/MIME, users must store public keys for every recipient to whom they send encrypted messages in their Outlook contacts. Outlook cannot use the S/MIME certificates stored for users in on-premises Active Directory because the Directory

Synchronization tool does not synchronize the Active Directory userSMIMECert attribute to Exchange Online.

- S/MIME is supported in Outlook but not in Outlook Web App. Customers are responsible for all public key infrastructure (PKI) and user S/MIME certificate enrollment.

- **Pretty Good Privacy (PGP) encryption:** Exchange Online transports and stores messages that are encrypted using client-side, third-party encryption solutions such as PGP. Exchange Online does not host public keys and does not provide key repository, key management, or key directory services.
- **Information Rights Management:** Exchange Online does not provide hosted Information Rights Management (IRM) services, but administrators can use on-premises Active Directory Rights Management Services in conjunction with Exchange Online. If an Active Directory Rights Management Services server is deployed, Outlook can directly communicate with the Active Directory Rights Management Services server, enabling users to compose and read messages protected by Active Directory Rights Management Services. Active Directory Rights Management Services server and Exchange Online do not require interoperability to use the Active Directory Rights Management Services features of Outlook. The following features become available:
  - Support for IRM in Outlook Web App
  - Support for IRM in Exchange ActiveSync
  - IRM search
  - Transport protection rules
  - Protected voice mail
  - Journal report decryption
  - Outlook protection rules
  - Role-Based Access Control

SharePoint Online Security

The SharePoint Online service is enabled through SharePoint Server 2010, which offers a wide range of security features, including:

- **Virus filtering:** Microsoft Forefront Security for SharePoint is included with SharePoint Online to help protect the SharePoint Online environment from viruses while maintaining uptime and optimizing performance. Forefront Security for SharePoint provides comprehensive protection for SharePoint document libraries using multiple scan engines and content controls to help eliminate documents that contain malicious code.
- **Blocked file types:** To protect computers from potentially harmful code, SharePoint Online blocks certain kinds of files from being uploaded to or retrieved from the SharePoint Online environment. Files are blocked on the basis of the file name extension, and SharePoint Online maintains a list of file name extensions that are blocked. (For example, .exe files are on the list of blocked file name extensions, so a file called "filename.exe." would be blocked.)

Note

This feature does not prevent all exploitations based on file types. For a list of blocked file name extensions, see Appendix: Blocked File Name Extensions.

- **Hosted protection:** SharePoint Online security measures include providing firewall protection, and intrusion detection for the systems hosted at the Microsoft data center.
- **Granular access control:** SharePoint Online uses a granular access control model to control access to the SharePoint Online service.
- **IRM:** While SharePoint Online does not yet integrate with an Information Rights Management server, it is possible to store a rights protected file in a SharePoint Online document library. Note: a rights protected document will not be crawled by the SharePoint Online search indexer.
- **Windows event log:** SharePoint Online events are logged in the Windows event log and are addressed by the SharePoint Online internal team only.
- **Software updates:** The Microsoft operation center team deploys software updates in order to maintain the highest level of security and software reliability. Software hotfixes and service packs are deployed based on their priority and level of risk. Security-related hotfixes are rapidly deployed into the environment to address current threats. A comprehensive software validation activity ensures software stability through regression testing prior to deployment.
- **Access control:** Microsoft provides three-tier administration for administering SharePoint Online, including:
  - Site-level administration: Content Administrators at this level can authorize the content changes.
  - Shared service administration: Shared Content Administrators at this level are responsible for service configuration and service authorization.
  - Central administration: IT administrators with access to central administration are authorized to apply security policies to SharePoint Online and to perform SharePoint farm configuration.
- **Authentication of an identity:** SharePoint Online uses the Microsoft NTLM (Windows Challenge/Response) authentication protocol to authenticate an identity that requests access to SharePoint data. The NTLM authentication protocol is dependent on the Net Logon service on domain controllers for client authentication and authorization information.
- **Microsoft Excel® Services security:** Excel Services in SharePoint Online is used to enable data visualization, perform calculations, and display components of Excel Workbook (like graphs, ranges, etc.) that are stored in SharePoint Online document libraries. The transmission of Excel Services data is secured at all levels using IPsec and SSL.

Lync Online Security

The Lync Online service is enabled through the Lync Server 2010 that offers a wide range of security features, including:

- **Instant messaging security:** Microsoft has extensive experience in designing and operating a highly available instant messaging (IM) solution. One key component is the Intelligent Instant Message Filter (IIMF) built into Lync Online, which helps protect both the customer network and the network managed by Microsoft against the spread of the most common viruses and spam. Subscribers to Lync Online benefit from an IIMF design that is built on years of operating scalable, global IM systems, which can help to protect users from malicious content and links transmitted using IM. Other security features that Lync Online provides include IM and media encryption and IM filtering.
- **IM federation:** IM federation enables Lync Online users to connect with other organizations that use Lync Online as well as those that host their own Lync Server 2010 on premises. Lync Online users can also federate with trusted users from the Windows® Live Messenger public IM network. All federated communications are encrypted between the IM systems using access proxy

servers. Microsoft does not control encryption after messages are passed to the federated partner network (if the partner is federated with an on-premises Lync Server 2010 or third-party network).

IM federation requires the consent and proper configuration of both parties of the federation relationship. Once the federation is set up by the administrators of both sides, users in each company can start seeing presence and communicating with users in the other company.

Note

Use of the term *federation* in the Lync Online context generally refers to Lync Online capabilities to communicate with other messaging systems and should not be confused with the requirements and capabilities of federated identities with Office 365.

Table 1 describes the supported communication features across federated link types:

Table 1: Federation features by link type

	IM and Presence	PC-to-PC Audio and Video
Lync Online tenants (other companies using Office 365 and Lync Online)	Yes	Yes
Lync Server 2010 on premises (any version)	Yes	Yes
Windows Live Messenger	Yes	No

Service administrators can control which systems are allowed to communicate with Lync Online users by using whitelists and blacklists.

Limit

- Federation requires DNS configurations by the customer and each federated partner organization. Federated organizations are solely responsible for proper configuration of their environments to support federation.
- Federated connections are not covered by the SLAs provided as a part of Office 365 subscriptions.
- Federated connections are excluded from the service continuity management recovery time objectives (RTO) and recovery point objectives (RPO).
- File transfer is not available with federated connections.

Office Professional Plus Security

Microsoft Office Professional Plus 2010 offers improved security features that help Office 365 customers to be more confident in safeguarding their data. With Office Professional Plus, organizations provide innovative business solutions without sacrificing the features critical to success, such as maintaining security and protection. Office Professional Plus includes the following security features:

- **Trusted Documents and Protected View:** The Trusted Documents and Protected View features of Office Professional Plus combine to provide better security against malicious email attachments

and files while simultaneously allowing users to quickly view documents. When users open documents that originate from an Internet source, they automatically open in Protected View.

- **Cryptographic Agility:** Office Professional Plus offers increased security with out-of-the-box support for Cryptographic Agility by integrating with the Cryptographic Next Generation (CNG) interfaces for Windows; administrators can specify cryptographic algorithms for encrypting and signing documents.
- **Additional security policies:** Office Professional Plus enables IT to enforce password and security consistency by ensuring that all Office documents conform to domain password complexity rules.
- **High-fidelity, consistent views:** Online users must be able to view content as it was created in desktop versions of Microsoft Office programs. Office Web Apps provide professional, high-fidelity companions to Microsoft Word, Excel, Microsoft PowerPoint®, and Microsoft OneNote®. Users can take advantage of the rich features in Microsoft Office on their desktops to create content and then share those files online with great document fidelity and consistent formatting.

Microsoft Office 365 Service Continuity

Service continuity management focuses on the ability to restore services for Office 365 customers in a predetermined timeframe during a critical service outage. Achieving restored services requires preparation, planning, technical implementation, exercises that simulate outages, and execution at the time of an incident.

This section describes the common approach to service continuity management that is taken by Office 365 across all of its services. It also explains how Office 365 ensures data availability and service reliability to customers. This section also explains how service continuity capabilities developed by Microsoft are integrated into the design of individual Office 365 services, including Exchange Online, SharePoint Online, Lync Online, and Office Professional Plus.

Service Continuity Management

Office 365 offerings are delivered by highly resilient systems that help to ensure high levels of service. Office 365 capitalizes on the experience that Microsoft has in hosting services as well as close ties to Microsoft product groups and support services to create a service that meets the high standards that customers demand.

Service continuity provisions are part of the Office 365 system design. These provisions enable Office 365 to recover quickly from unexpected events such as hardware or application failure, data corruption, or other incidents that affect users. These service continuity solutions also apply during catastrophic outages (for example, natural disasters or a fire within a Microsoft data center that renders the entire data center inoperable).

Incident Classification

Service outages may be caused by hardware or software failure in the Microsoft data center, a faulty network connection between the customer and Microsoft, or a major data center challenge such as fire, flood, or regional catastrophe. Most service outage incidents can be addressed using Microsoft technology and process solutions and are resolved within a short time. However, some incidents are more serious and can lead to long-term outages.

Office 365 uses the Service Interruption Scale (see Figure 1), which classifies outage incidents as minor, critical, and catastrophic events based on their impact to customers.

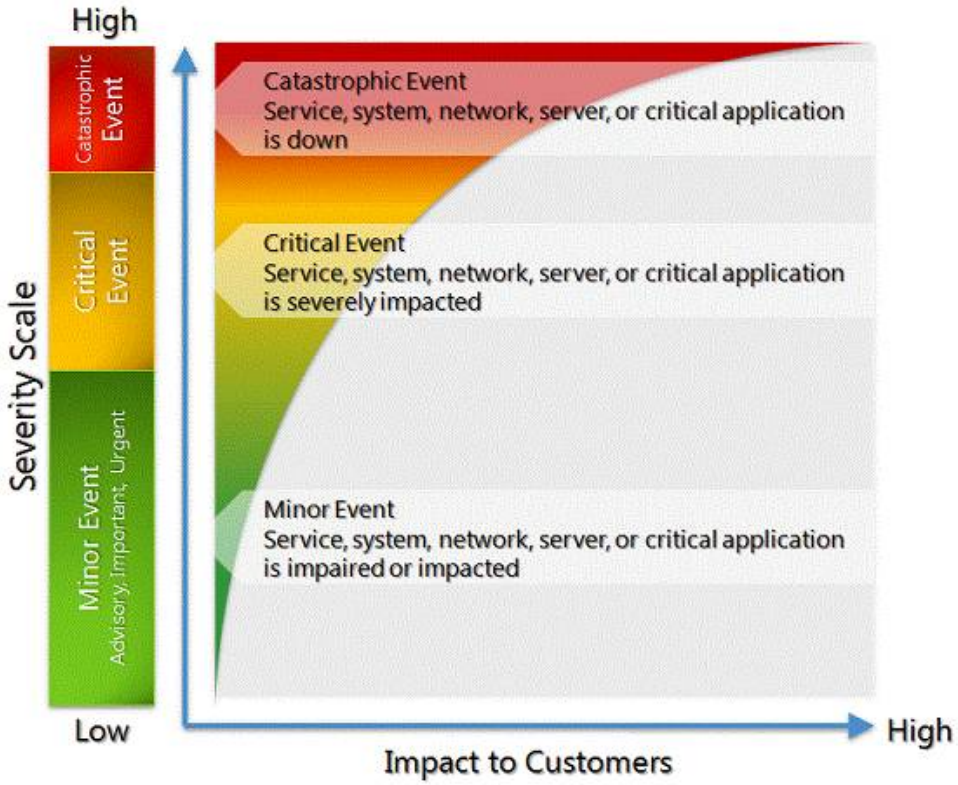

Figure 1. Service Interruption Scale

Catastrophic Outage Response

Office 365 analyzes each incident that affects service availability to determine scope and possible solutions. Outages that cause customer work to stop may be considered catastrophic outages. In the event of a catastrophic outage, the Office 365 incident management team sends the initial outage notification to the customer via email unless the customer's email service is not functional; in that case, a phone call is made to an agreed-on customer telephone number. Status updates are provided to the customer every hour or as appropriate for the particular incident.

Disaster Declaration

Outages that are classified as a critical or catastrophic event based on the Service Interruption Scale may be declared disasters. When an outage is declared a disaster, regular customer notifications are provided by the Office 365 incident management organization until a solution is found.

Declaration of a disaster does not automatically result in failover of the customer's redundant secondary site.

Customer Responsibilities

- **Provide contact information:** Provide a single email group alias and phone number so that Microsoft can engage appropriate personnel at the time of an event to review the current status of the outage, disaster declaration criteria, and approval or disapproval of failing over to the secondary site.
- **Provide declaration support:** Provide an executive-level contact to the Microsoft declaration authority to help determine if failover to the customer secondary site is necessary.

Microsoft Responsibilities

- **Provide contact information:** Provide a single email group alias and phone number so that the customer can engage appropriate personnel at the time of an event to review current status of the outage, disaster declaration criteria, and approval or disapproval of failing over to the secondary site.
- **Decide whether failover is required:** Incorporate feedback from the customer to decide whether to fail over to the customer secondary site.

Ensuring Data Availability

Microsoft ensures customer data is available whenever it is needed, with the help of the following features of Office 365 services.

Data Storage and Redundancy

Customers' data is stored in a redundant environment with robust backup, restore, and failover capabilities to enable availability, business continuity, and rapid recovery. Multiple levels of data redundancy are implemented, ranging from redundant disks to guard against local disk failure to continuous, full data replication to a geographically diverse data center.

Data Monitoring and Maintenance

Along with avoiding data loss, Office 365 helps maintain data performance.

- **Monitoring databases:** Databases are regularly checked for:
  - Blocked processes.
  - Packet loss.
  - Queued processes.
  - Query latency.
- **Preventative maintenance:** Maintenance includes database consistency checks, periodic data compression, and error log reviews.

Dedicated Support

The Office 365 development and operations teams are complemented by a dedicated Office 365 support organization, which plays an important role in providing customers with business continuity. Support staff has a deep knowledge of the service and its associated applications as well as direct access to Microsoft experts in architecture, development, and testing.

The support organization closely aligns with operations and product development, offers fast resolution times and provides a channel for customers' voices to be heard. Feedback from customers provides input to the planning, development, and operations processes.

- **Online issue tracking:** Customers need to know that their issues are being addressed, and they need to be able to track timely resolution. The Office 365 Portal provides a single web-based interface for support. Customers can use the portal to add and monitor service requests and receive feedback from Microsoft support teams.
- **Self-help, backed by continuous staff support:** Office 365 offers a wide range of self-help resources and tools that can help customers to resolve service-related issues without requiring Microsoft support.

Before customers enter service requests, they can access knowledge base articles and FAQs that provide immediate help with the most common problems. These resources are continually updated with the latest information, which helps avoid delays by providing solutions to known issues. However, when an issue arises that needs the help of a support professional; staff members are available for immediate assistance by telephone and via the administration portal 24 hours a day, 7 days a week.

SharePoint Online Continuity

The availability of customer data stored on SharePoint Online is ensured through:

- **Data backup:** Data protection services help prevent the loss of SharePoint Online data. Backups are performed every 12 hours and retained for 14 days.
- **Meeting service recovery level:** Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) have been set to minimize loss of data and time to service restoration in case of a disaster. Please see the SharePoint Online Service Description document for more information.

Microsoft Office 365 Compliance

Microsoft has designed security, data protection, reliability, and privacy of Office 365 services around high industry standards Office 365 and the infrastructure on which it relies (Microsoft Global Foundation Services) employ security frameworks based on the International Standards Organization (ISO/IEC 27001:2005) family of standards and are ISO 27001 certified by independent auditors. Our ISO 27001 certifications enable customers to evaluate how Microsoft meets or exceeds the standards and implementation guidance against which we are certified. BSI auditing professionals are bound by professional ethics to provide an unbiased, third-party analysis of Office 365 compliance. To make this evaluation, they observe routine operations, interview relevant personnel, and review documentation in each of the areas covered in the Statement of Applicability (SOA). ISO 27001 defines how to implement, monitor, maintain, and continually improve the Information Security Management System (ISMS). In addition, both the services and the infrastructure undergo a yearly SAS 70 (or successor SSAE16) assessments.

The Microsoft Online Services Information Security Policy, applicable to Office 365, aligns with International Organization for Standards ISO 27002 augmented with requirements specific to online services. The ISO 27001 certification which Microsoft has received is supplemented by ISO 27002, which provides a suggested set of suitable controls.

Office 365 customers can review the ISO standard and published Microsoft services documentation to determine whether their security requirements are satisfied. Office 365 features enhanced security for most types of data and jurisdictions. However, customers must evaluate sensitive data, or data that must be held to a certain level of security or under applicable regulations, for use through the service offering. In some instances, the data may require a specific security requirement that Microsoft does not provide.

Support for Leading Industry Certifications

Microsoft was first certified for Safe Harbor in 2001, and the LCA Regulatory Affairs team recertifies compliance with the Safe Harbor Principles every twelve months.

In addition to the EU Member States, members of the European Economic Area (Iceland, Norway, and Liechtenstein) also recognize Safe Harbor members as providing adequate privacy protection to justify trans-border transfers from their countries to the U.S. Switzerland has a nearly identical agreement (Swiss-U.S. Safe Harbor) with the U.S. Department of Commerce to legitimize transfers from Switzerland to the U.S., to which Microsoft has also certified. Several other countries, such as Canada and Argentina, have passed comprehensive privacy laws and the EU has cleared them for data transfer from the EU to those countries.

The Gramm Leach Bliley Act (GLBA) sets minimum security and privacy requirements for financial institutions in the United States. Software/ services cannot claim to be "GLBA compliant" because GLBA compliance also requires procedures and policies. Two of the principal regulations under GLBA that affect Microsoft Office 365 cloud services are:

- **Financial Privacy Rule**: Governs the collection and disclosure of customers' personal financial information by financial institutions
- **Safeguards Rule**: Requires all financial institutions to design, implement, and maintain safeguards to protect customer information, whether they collect such information themselves or receive it from other financial institutions.

Office 365 ordering, billing, and payment systems that handle credit card data are Level One Payment

Card Industry (PCI) Compliant, and customers can use credit cards to pay for the services with confidence. An independent third party audits and determines whether the Microsoft Online Commerce Platform (OCP) which supports Office 365 has satisfactorily met the Payment Card Industry Data Security Standard (PCI DSS) version 1.2.

Office 365 services are not suitable for processing, transmitting, or storing PCI-governed data. PCI-DSS is an industry standard designed to protect and maintain sensitive data during transmission and storage throughout the data life cycle. At a minimum, organizations that support transactions via credit and debit cards are required to have a degree of compliance to the PCI standard.

There is much confusion in the marketplace around the impact of PCI DSS; many customers state that all data within their organizations requires PCI certification and compliance, and the Microsoft Online Services must also demonstrate compliance. While it is true that Microsoft Online Services needs to be compliant for the Primary Account Number (PAN) data it processes, and it is, customers should not use the Office 365 service to transmit or store PAN data for their own use.

Note

PCI compliance will only apply if Primary Account Number (PAN) is transmitted or stored within the online environment. To be compliant, the PAN data must be encrypted during transmission and storage. In addition, reporting must demonstrate that this encryption has successfully protected the PAN data. As a result, the service is not a suitable storage medium for PAN data, and companies should apply customer-side policies to prevent the transmission of PAN data to the online environment.

Appendix A: Blocked File Name Extensions

Table A1 shows the file name extensions that are blocked in SharePoint Online.

Table A1: Blocked file name extensions

Extension	File type
.app	Application file
.bas	Microsoft Visual Basic class module
.bat	Batch file
.chm	Compiled HTML Help file
.class	Java class file
.cod	Windows NT Command Script
.com	Microsoft MS-DOS program
.cal	Control Panel extension
.crt	Security certificate
.dll	Windows dynamic link library
.exe	Executable program
.fxp	Microsoft Visual FoxPro compiled program
.hlp	Help file
.hta	HTML application
.ins	Internet Naming Service
.isp	Internet Communication settings
.jse	JScript Encoded script file
.lnk	Shortcut
.mda	Microsoft Access add-in program
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.mdt	Microsoft Access data file
.mdw	Microsoft Access workgroup
.mdz	Microsoft Access wizard program
.msc	Microsoft Common Console document
.msi	Windows Installer package
.msp	Windows Installer patch
.mst	Microsoft Visual Test source files
.ops	Microsoft Office profile settings file
.pcd	Photo CD image or Visual Test compiled script
.pif	Shortcut to MS-DOS program
.prf	System file
.prg	Visual FoxPro source file
.reg	Registration entries

Extension	File type
.scf	Windows Explorer command file
.scr	Screen saver
.sct	Windows Script Component
.shb	Windows shortcut
.shs	Shell Scrap object
.url	Uniform Resource Locator (Internet shortcut)
.vb	Visual Basic script file
.vbe	Visual Basic Scripting Edition Encoded script file
.vbs	Visual Basic Scripting Edition file
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file