Microsoft®
Online Services

Microsoft Online Services Controls as Aligned to ISO/IEC 27001:2013 with ISO/IEC 27018:2014

The Microsoft Online Services Responses in this document are generalized, plain language representations of the control implementation and are not intended to supplant the actual engineering implementation details.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication and is subject to change at any time without notice to you. This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. This document is confidential and proprietary to Microsoft. It is disclosed and can be used only pursuant to a non-disclosure agreement.

Document type: Controlled (handed to customer under NDA when authenticated or on request)
Document stage: Published
Next review: November 2015

INTRODUCTION

Microsoft Online Services provides subscription-based enterprise software services hosted by Microsoft. Our software services, Business Productivity Online Suite Standard, Dedicated and Office 365, are infused with standards and features that reflect the strategic needs and competitive demands of global businesses. As a result, customers continually benefit from the latest technologies and improvements.

Microsoft Online Services' security architecture embodies the key principles of the Microsoft Trustworthy Computing initiative: protection of sensitive data, adherence to business practices that promote trust with users, and a focus on solid engineering and best practices to ensure the delivered product or service is reliable and secure.

Developed for global enterprises, Microsoft Online Services' multi-faceted security program applies a common set of security policies to manage risk and mitigate threats to customer data. Microsoft is able to continually improve security by standardizing the way we test, implement, and monitor policies for all of our customers. In turn, each Microsoft Online Services customer benefits from Microsoft's experience with the security issues of customers all over the world — and from the practices Microsoft applies to address them.

Microsoft Online Services recognizes how important it is that our customers understand the means by which we mitigate risks to their vital services and data. The scope of this document primarily focuses on addressing questions regarding centralized risk management controls that underpin service level or application risk management functionality. The control categories and questions addressed by Microsoft Online Services are based on ISO/IEC 27001:2013 which establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. Rare but valid exceptions to the processes and controls listed below occur in services from time to time; these exceptions originate mostly from engineering and operational reasons and are carefully tracked and reviewed by management. It is also important to note that some of these controls are managed by areas outside of the Microsoft Online Services Platform and thus are not directly covered in the ISO audit.

Document type: Controlled (handed to customer under NDA when authenticated or on request)
Document stage: Published
Next review: November 2015

CONTENTS

Document type: Controlled (handed to customer under NDA when authenticated or on request)
Document stage: Published
Next review: November 2015

ISO/IEC 27001:2013 CONTROLS

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Online Services Response
A.5 INFORMATION SECURITY POLICIES		
A.5.1 MANAGEMENT DIRECTION FOR INFORMATION SECURITY		
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Microsoft develops, documents, and disseminates a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The Microsoft Security Policy exists in order to provide Microsoft Services Staff and Contractor Staff with a current set of clear and concise Information Security Policies. These policies provide direction for the appropriate protection of the Microsoft Services. The Microsoft Security Policy has been created as a component of an overall Information Security Management System (ISMS) for the Microsoft Services. The Microsoft Security Policy has been reviewed, approved, and is endorsed by Microsoft Online Services management. Each management-endorsed version of the Microsoft Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Microsoft Security Policy is made available to all new and existing Microsoft Services Staff for review. All Microsoft Services Staff represent that they have reviewed, and agree to adhere to, all policies within the Microsoft Security Policy documents. All Microsoft Services Contractor Staff agree to adhere to the relevant policies within the Microsoft Security Policy. Should one of these parties not have access to this policy for any reason, the supervising Microsoft agent is responsible for distributing the policy to them. A customer facing version of the Microsoft Security Policy is made available for customer review through escalation to account or support representative. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Policy.

<table>
<tr><th>ISO/IEC 27001:2013 Control ID</th><th>ISO/IEC 27001:2013 Control</th><th>Microsoft Online Services Response</th></tr>
<tr><td>A.5.1.2</td><td>The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.</td><td>Microsoft regularly reviews and updates the current security awareness and training policy.
The Microsoft Security Policy undergoes a formal review and update process at a regularly scheduled interval not to exceed 1 year. In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule.</td></tr>
<tr><td colspan="3">A.6 ORGANIZATION OF INFORMATION SECURITY</td></tr>
<tr><td colspan="3">A.6.1 INTERNAL ORGANIZATION</td></tr>
<tr><td colspan="3">Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.</td></tr>
<tr><td>A.6.1.1</td><td>All information security responsibilities shall be defined and allocated.</td><td>Microsoft identifies individuals having information system security roles and responsibilities.
The Microsoft Security Policy defines Microsoft policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Services. The Microsoft Security Policy addresses roles, responsibilities, management commitment, coordination among organizational entities, and compliance with the policy. The Microsoft Security Policy contains rules and requirements that must be met in the delivery and operation of Microsoft Services.
The Microsoft Security Policy applies across the company to all information and processes used in the conduct of Microsoft business. All Microsoft employees and contingent staff are accountable and responsible for complying with these guiding principles within their designated roles.
Consistent with Policy, hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background characteristics needed to perform the job, and personal characteristics required. Once the requirements are determined, managers create a job description, which is a profile of the job and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make an appropriate hiring decision.</td></tr>
</table>

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Online Services Response
A.6.1.2	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Microsoft separates duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. All Microsoft service teams have defined roles as part of a comprehensive role-based access control mechanism. Additionally, each service team has identified any roles that, if shared by a single person, would allow for malicious activity without collusion. If such roles exist, no individual is allowed to belong to both roles. As one example, throughout Microsoft Online Services, any individual in a role that has permissions to modify or delete audit records cannot share a role that has permissions to production services. This prevents a single Microsoft user from performing a malicious action and then removing evidence of having performed that action.
A.6.1.3	Appropriate contacts with relevant authorities shall be maintained.	Microsoft identifies individuals having information system security roles and responsibilities. Microsoft Services partners with the Microsoft Trustworthy Computing Group to maintain contact with external parties such as regulatory bodies, service providers, and industry forums to ensure appropriate action can be quickly taken and advice obtained when necessary. We rely on the Global Criminal Compliance (GCC) & LCA organization for most contacts with law enforcement. Roles and responsibilities for managing and maintaining these relationships are defined.
A.6.1.4	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Microsoft establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel. Microsoft Services partners with the Microsoft Trustworthy Computing Group to maintain contact with external parties such as regulatory bodies, service providers, and industry forums to ensure appropriate action can be quickly taken and advice obtained when necessary. We rely on the Global Criminal Compliance (GCC) & LCA organization for most contacts with law enforcement. Roles and responsibilities for managing and maintaining these relationships are defined.

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Online Services Response
A.6.1.5	Information security shall be addressed in project management, regardless of the type of the project.	Microsoft addresses Information security in project management, regardless of the type of the project. Microsoft's implementation of life cycle support is outlined through Microsoft Security Development Lifecycle (SDL), (SDL) process that is followed by all engineering and development projects. A security requirements analysis must be completed for all system development projects. This analysis document acts as a framework and includes the identification of possible risks to the finished development project as well as mitigation strategies which can be implemented and tested during the development phases. Critical security review and approval checkpoints are included during the system development life cycle.
A.6.2 MOBILE DEVICES AND TELEWORKING		
Objective: To ensure the security of teleworking and use of mobile devices.		
A.6.2.1	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Microsoft has adopted a policy and supporting security measures to manage the risks introduced by using mobile devices Unauthorized mobile computing devices are not permitted in, or directly attached to, any Microsoft Online Services production environment. The Organization's staff and contingent staff must adopt and follow appropriate security practices when using mobile computing devices to protect against the risks of using mobile equipment. Such risks relate to the mobile nature of these devices, and the security practices adopted by Microsoft to mitigate these risks may include, but are not limited to, mobile device physical protection, access controls, cryptographic requirements, virus protection, and/or locations the devices may be coming from. Mobile computing devices may not be directly attached to, any of the Microsoft's production environments, unless those devices have been approved for use by Microsoft's management. Mobile computing and data recording devices are not to be used in any of Microsoft's services production environments without prior approval by the Data Center Management Team via an access request. Mobile computing and data recording devices include PDAs, portable hard drives, laptop computers, flash drives, other recordable media, etc. Microsoft monitors for all

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Online Services Response
		unauthorized use of mobile devices in the Microsoft Online Services environment and performs investigations accordingly. All Microsoft Online Services assets are locked in cages in Microsoft facilities that are access-controlled. While Microsoft Online Services technicians have physical access to the servers within the cages, they do not have the logical access to the servers that would be required to make use of portable media.
A.6.2.2	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Microsoft employs a policy and supporting security measures to protect information accessed, processed or stored at teleworking sites. Telecommunicating locations are governed by the Microsoft remote access policy which requires remote access to production Microsoft's online services' networks to employ authentication mechanisms.

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response

A.7 HUMAN RESOURCE SECURITY

A.7.1 PRIOR TO EMPLOYMENT

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
A.7.1.1	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Microsoft screens individuals prior to authorizing access to the information system. Microsoft has implemented the personnel screening control through the use of background checks on employees and contractors. The Microsoft Online Services Standards states that new employees (full time employees and contingent staff) are subject to a background check as part of the normal Microsoft Human Resources hiring practices. No candidate or employee will begin work or be placed on an assignment until the required background checks have been successfully completed. Certain roles, supporting cloud offerings may involve additional background checks or authentication requirements, such

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		as proof of United States citizenship, or personnel security clearances which may require fingerprinting. Background checks are required when hiring domestic external candidates as well as for current employees and internal transfers, whose jobs include working on customers' worksites and/or having access to certain sensitive areas, including potential access to customer personally identifiable information (PII) as defined in the Microsoft Asset Classification & Protection Standard. Any job-related criminal history or material misrepresentation, falsification, or omission of fact may disqualify a candidate from employment or, if the individual has commenced employment, may result in termination of employment at a later date.
A.7.1.2	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Microsoft ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access. All Microsoft Online Services staff are required to sign confidentiality and non-disclosure agreements, as well as the Microsoft Employee Handbook, at the time of hire as a condition for employment. Additionally, the Microsoft Corporate General Use Standard describes user responsibilities and establishes expected behavior when using Microsoft Online Services. All users, including employees, vendors, and contractors are required to follow the rules of behavior outlined in the General Use Standard. Vendors and contractors are required to have a signed Microsoft Master Vendor Agreement (MMVA) to ensure compliance with Microsoft policies on required engagements. The agreements are put in place to protect trade secrets, sensitive, or business confidential information and assets. All Microsoft's Online Services contingent staff must also sign a non-disclosure agreement at the time of engagement and before being given access to Microsoft's Online Services.
A.7.2 DURING EMPLOYMENT		
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.		
A.7.2.1	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Microsoft receives a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		Microsoft's Corporate IT Policy applies across the company to all information and processes used in the conduct of Microsoft business. All employees, interns, vendors, contingent staff, partners, and business guests are accountable and responsible for complying with these guiding principles. Additionally, all Microsoft staff are required to comply with the Microsoft Security Policy and Standards. This includes those located at Microsoft subsidiaries and locations not owned by Microsoft such as offsite facilities.
A.7.2.2	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Microsoft provides role-based security training to personnel with assigned security roles and responsibilities when required by information system changes. All appropriate Microsoft Staff take part in a Microsoft Online Services sponsored security-training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. All Microsoft Online Services Contractor Staff are required to take any training determined to be appropriate to the services being provided and the role they perform. All staff are required to enroll in a New Employee Orientation (NEO) security awareness training course, Standards of Business Conduct, within the first 30 days of their employment or transfer into the organization. Microsoft Online Services Risk Management has implemented the security training control by requiring all new users (employees and contractors) to take the initial security and awareness training on an annual basis. Non-operational personnel, anyone that is involved in development and quality assurance, are also required to take the mandatory training offered by Online Services Security, as well as training associated with the Operational SOPs related to Asset Handling, Incident Response, and Change Control. In addition, training related to the system being accessed, along with associated procedures, may be required. Security training is also required when there is a significant change to the system environment.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.7.2.3	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Microsoft employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. Microsoft Online Services staff suspected of committing breaches of security and/or violating Microsoft Security Policy equivalent to a Microsoft Code of Conduct violation are subject to an investigation process and appropriate disciplinary action up to and including termination. Contractor Staff suspected of committing breaches of security and/or violation of Microsoft Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts. Once a determination has been made that Microsoft Online Services Staff has violated Policy, Human Resources is informed, and is responsible for coordinating disciplinary response.

A.7.3 TERMINATION AND CHANGE OF EMPLOYMENT

Objective: To protect the organization’s interests as part of the process of changing or terminating employment.

A.7.3.1	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Microsoft, upon termination of individual employment conducts exit interviews that include a discussion of information security topics. Responsibilities of management and employees related to completing the terminations including revocation of access, return of smartcards, ID cards, equipment and documentation, etc. are formally documented, and communicated by HR.

A.8 ASSET MANAGEMENT

A.8.1 RESPONSIBILITY FOR ASSETS

Objective: To identify organizational assets and define appropriate protection responsibilities.

A.8.1.1	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Microsoft develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting. Microsoft Online Services has implemented a formal policy that requires major assets used to provide Microsoft Online Services to be accounted for and have a designated asset owner. An inventory of major hardware assets in the Microsoft Online Services

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		environment is maintained in an asset management tool. Asset owners are responsible for maintaining up-to-date information regarding their assets within the asset inventory including owner or any associated agent, location, and security classification. Asset owners are also responsible for classifying and maintaining the protection of their assets in accordance with the standards. The Asset Management team maintains portions of the hardware asset data on behalf of the asset owner or associated agent and updates certain attributes in the asset management tool such as asset tag, physical location, etc.
A.8.1.2	Assets maintained in the inventory shall be owned.	Microsoft develops and documents an inventory of information system components that accurately reflects the current information system. The Asset Management team uses a centralized ticketing system to track the service team requests and movement of assets. Assets have an assigned owner and policies and procedures have been developed and implemented to define owner responsibilities.
A.8.1.3	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Microsoft regularly reviews and updates the rules of acceptable usage standards of the Infrastructure & Services technology assets. The Microsoft Online Services Acceptable Use Policy outlines the Online Services specific acceptable usage standards of the Infrastructure & Services technology assets. Additionally, the Microsoft General Use Standard describes user responsibilities and establishes expected behavior when using Microsoft Online Services and other Microsoft systems. All users, including employees, vendors, and contractors are required to follow the rules of behavior, which are outlined in the Microsoft General Use Standard. The agreements are put in place to protect trade secrets, sensitive, or business confidential information and assets. The NDA, Employee Handbook, and Microsoft Security Policy include statements regarding information and asset protection responsibilities. They also describe the penalties for the violation of these responsibilities.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.8.1.4	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Microsoft, upon termination of individual employment, retrieves all security-related organizational information system-related property. Human Resources Assistants or the employee's manager collect Microsoft badges at the time of the exit interview or termination. Business Administrators and/or managers of the terminated employee collect hardware assets. Microsoft may also conduct an audit to make sure data is removed in an appropriate manner.
A.8.2 INFORMATION CLASSIFICATION		
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.		
A.8.2.1	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	Microsoft categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Standards provide guidance for classifying assets into one of the following security classification categories • High Business Impact (HBI) • Moderate Business Impact (MBI) • Low Business Impact (LBI) The Asset Owner/Trustee classifies all of their Assets into one of these categories. The Asset Owner/Trustee then classifies the data as either customer data or Microsoft data, and applies additional security attributes to customer data, based on the category above. Microsoft Online Services has completed a Certification and Accreditation (C&A) package to be authorized to operate at FIPS 199 Moderate impact level. Based on FIPS 199 standards, Microsoft Online Services service teams identified a selection of user and system information types based on system components within Microsoft Online Services core offerings. Utilizing this selection, Microsoft categorized information types and evaluated the impact on the organization from compromise of confidentiality, loss of integrity or lack of availability (CIA).

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.8.2.2	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Microsoft policy requires that Information Assets must be protected based upon their classification and according to the Asset Protection Standard. Assets within Microsoft data centers are marked with a HBI, MBI, or LBI (High, Moderate, or Low Business Impact) designation which requires different levels of security and handling precautions. Asset owners are required to classify their assets that are stored within a data center. Asset owners are required to assign their assets an asset classification and no assets are exempt from this requirement. In the data center environment, assets refer to servers, network devices, and magnetic tapes. Other digital media like USB flash/thumb drives, external/removable hard drives, or CD/DVD's are not used. Non-digital media is not used in the data center.
A.8.2.3	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Microsoft restricts access to digital media to organization-defined personnel or roles. Microsoft has implemented media access through the implementation of Microsoft Security Policy. Logical access to digital media is controlled via Active Directory Group Policy Objects (AD GPOs) and security groups. Physical access to all media is restricted by the data center access process. Access is restricted to individuals who have a legitimate business purpose for accessing the data. The Asset Protection Standard defines the safeguards required to protect the confidentiality, integrity, and availability of information assets within Microsoft data centers.
A.8.3 MEDIA HANDLING		
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.		
A.8.3.1	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Microsoft develops, documents, and disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the media protection policy and associated media protection controls. Microsoft doesn't use removable media within the service or for backups. Instead, the Microsoft Online Services are designed so that all backups are done through directly attached storage devices rather than by removable disks.
A.8.3.2	Media shall be disposed of securely when no longer required, using formal procedures.	Microsoft sanitizes media prior to disposal, release out of organizational control, or release for reuse using in

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		accordance with applicable federal and organizational standards and policies. Microsoft maintains accountability for assets leaving the data center through the use of NIST SP 800-88 consistent cleansing/purging, asset destruction, encryption, accurate inventorying, tracking, and protection of chain of custody during transport.
A.8.3.3	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Microsoft protects and controls data on storage media during transport outside of controlled areas. For this control, digital media at Microsoft data centers consist of servers, network devices, and magnetic backup tapes. Microsoft data centers do not use non-digital media. Microsoft utilizes 3 methods to protect media that is being transported outside the data center: 1) Secure Transport 2) Encryption 3) Cleanse, Purge, or Destroy. 1. All media being transported from Microsoft data centers require accurate tracking. Tickets are created to arrange and track the transportation of media. Microsoft has contracted with several approved vendors to provide secure shipping services. Secure Transport begins with an accurate inventory and chain of custody. Authorized asset managers are required to manage the exchange of assets. Assets are inventoried at the time of delivery to the transporter. The asset manager must witness the container being locked and a tamper proof seal applied. Secure Transport could have additional requirements such as a dedicated transport for only Microsoft assets, GPS tracking, and only stopping at Microsoft locations. In cases of longer transport routes, the requirement could be that there are multiple drivers and trucks with sleeping quarters to provide for non-stop delivery. At the delivery location, the transport company's approved personnel must be present to witness the removal of the tamper proof seal and unlocking of the container. The receiving personnel will inventory the shipment and send a message confirming the receipt of the assets. This inventory is validated by the Microsoft asset manager. 2. Some assets are required by Microsoft to be encrypted during transport. Magnetic backup tapes are

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		required to be encrypted. DPS utilizes SafeNet KeySecure to manage cryptographic keys using a FIPS 140-2 Level 3 validated encryption module (cert# 1694) and HSM (cert#1178) to secure AES 256-bit encrypted data on the magnetic tapes. When magnetic tapes are picked up for offsite storage, an approved asset manager must deliver the locked container to the offsite storage vendor and enter an account pin before inventorying the tapes being transported. Upon receipt of by the storage vendor, a message confirming the inventory received is sent to the asset manager. 3. Microsoft contracts with a vendor to provide equipment destruction. Depending on Microsoft asset classification some equipment is required to be destroyed onsite. All Microsoft assets are required to be cleansed or purged before leaving the data center Microsoft assets are cleansed/purged with methods consistent with NIST SP 800-88 prior to reuse or disposal. Microsoft utilizes data erasure units from Extreme Protocol Solutions (EPS). EPS software supports NIST SP 800-88 requirements for cleansing and purging/secure erasure. Prior to cleansing or destruction, an inventory is created by the Microsoft asset manager. If a vendor is used for destruction, the vendor provides a certificate of destruction for each asset destroyed, which is validated by the asset manager.
A.9 ACCESS CONTROL		
A.9.1 BUSINESS REQUIREMENTS OF ACCESS CONTROL		
Objective: To limit access to information and information processing facilities.		
A.9.1.1	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Microsoft develops, documents, and disseminates an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The Microsoft Security Policy defines Microsoft Online Services policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		organizations providing some level of support for the security of Microsoft Online Services. The Microsoft Security Policy addresses roles, responsibilities, management commitment, coordination among organizational entities, and compliance with the policy. Policies and procedures are distributed to personnel with responsibilities for implementing those policies and procedures via email links to SharePoint. Access control policy is a component of overall policies and undergoes a formal review and update process.
A.9.1.2	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Microsoft employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. By default, no one has access to customer content without authorization. When a problem arises or a customer requests a service ticket, a Microsoft administrator must use a special lockbox tool to request and obtain elevated privileges to enter the data system and fix the problem. The lockbox sits between the administrator and the customer's system. The lockbox tool checks the scope of the administrator's permissions for carrying out certain activities. The tool will approve or deny the request and, if approved, grant access only after management approval has also been obtained. In certain situations, the lockbox may also call to another administrator to assist with situation. Only absolutely necessary actions are permitted, and access is granted on a time-limited basis. After the permitted entry period has timed out, access privileges are automatically revoked. Every request for elevated privileges is logged.
A.9.2 USER ACCESS MANAGEMENT		
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.		
A.9.2.1	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Microsoft specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account. Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		The Microsoft Security Policy prohibits the use of guest/anonymous and temporary accounts. All account requests go through the standard account management process. Account changes are managed with automated workflow management tools that allow service teams to track the process through account request, approval, creation, modification, and deletion. From a people and process standpoint, Microsoft's presume breach practices involves 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) of engineer privileges to troubleshoot the service. An access approver role reviews and approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed.
A.9.2.2	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Microsoft creates, enables, modifies, disables, and removes information system accounts in accordance with the Microsoft Security Policy. The Microsoft Security Policy prohibits the use of guest/anonymous and temporary accounts. All account requests go through the standard account management process. Account changes are managed with automated workflow management tools that allow service teams to track the process through account request, approval, creation, modification, and deletion.
A.9.2.3	The allocation and use of privileged access rights shall be restricted and controlled.	Microsoft restricts privileged accounts on the system to defined personnel or roles. Microsoft Online Service teams require all individuals with administrative privileges to use their assigned accounts for performing business and administrative functions in the production environment. Microsoft Online Services requires that users of information system accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions. The Active Directory uses Role Based Access Control (RBAC) to enforce the separation of privileged and non-privileged roles.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.9.2.4	The allocation of secret authentication information shall be controlled through a formal management process.	Microsoft manages information system authenticators by establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators. The Microsoft Online Services manager of the Microsoft Online Services employee receives a onetime password from which is confidentially communicated to the Microsoft Online Services employee. At initial login, the employee is required to change their password in compliance with password design criteria. Regular system enforced password updates are made based on policy.
A.9.2.5	Asset owners shall review users' access rights at regular intervals.	Microsoft reviews accounts for compliance with account management requirements. The service team reviews accounts at least annually. A ticket is opened for each security group and the security group owner reviews membership for accuracy. If any discrepancies are found, they are noted in the ticket and a change is initiated in the account management tool.
A.9.2.6	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Microsoft, upon termination of individual employment disables information system access. Microsoft Human Resources (HR) holds the primary responsibility of ensuring personnel termination is handled appropriately. Account changes are managed through automated workflow management tools that allow service teams to track the process through account request, approval, creation, modification, and deletion. When an employee is terminated from Microsoft, the employee is removed from the system via a Termination Transaction. Once the transaction has been keyed in and approved, Microsoft Accounts and Security teams are notified and access to the network and buildings is shut off, via the termination transaction process and/or urgent terminations email template. For involuntary terminations, an urgent request for access termination is submitted via email from HR and access is disabled.

A.9.3 USER RESPONSIBILITIES

Objective: To make users accountable for safeguarding their authentication information.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.9.3.1	Users shall be required to follow the organization’s practices in the use of secret authentication information.	Microsoft manages information system authenticators by requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators. Microsoft enforces a minimum password complexity, password minimum and maximum lifetime restrictions, encrypts passwords in storage and in transmission, and prohibits password reuse. Passwords must not be shared or revealed to anyone other than the authorized Microsoft user and must be encrypted when stored. Additionally, passwords must be promptly changed if they are suspected of being known by unauthorized individuals. Authenticators must not be written down or stored in readable form batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them.
A.9.4 SYSTEM AND APPLICATION ACCESS CONTROL		
Objective: To prevent unauthorized access to systems and applications.		
A.9.4.1	Access to information and application system functions shall be restricted in accordance with the access control policy.	Microsoft system enforces mandatory access control over all subjects and objects where the policy specifies that the policy is uniformly enforced across all subjects and objects within the boundary of the information system. All Microsoft accounts are considered privileged. Each Microsoft administrator is assigned a role within their service team that corresponds to a security group. Each security group is assigned permissions to correlating environments with just enough access to properly fulfill their tasks. Service teams employ the concept of least privilege, allowing only pre-authorized accesses for users which are necessary to accomplish assigned tasks in accordance with business functions and organizational need. Service owners employ the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to operational assets, individuals, and/or other organizations.
A.9.4.2	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Microsoft uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		Microsoft Online Services properties uniquely identify and authenticate Microsoft organizational users through the use of multiple Active Directory deployments. Operations staff needing to perform administrative functions must access the environment remotely by design. Operations staff are identified by the Active Directory username specific to each property's environment, and authenticate using a strong password or two factor authentication. Microsoft Online Services implements authenticator feedback through the use of the built in operating system security controls that protect passwords when authenticating to system components. Passwords are obfuscated during the login process. No feedback is provided during the authentication process that could lead to potential exploitation by unauthorized users. Microsoft Online Services has policies that define session time-out requirements.
A.9.4.3	Password management systems shall be interactive and shall ensure quality passwords.	Microsoft, for password-based authentication, enforces minimum password complexity of case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type. Microsoft Online Services uses Active Directory to manage enforcement of our password policy. Microsoft Online Services systems are configured to force users to use complex passwords. Passwords are assigned a maximum age, a minimum length of characters. Password handling requirements include the changing of contractor supplied default passwords prior to introducing the associated service or system into any Microsoft Online Services owned or operated environment. Each Service Team within Microsoft Online Services has a local administrator password manager to securely maintain and store local administrator passwords for service systems.
A.9.4.4	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Microsoft requires that users of information system accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts or roles, when accessing non-security functions.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		No non-privileged actions (for example, use of web browsers, email clients, etc.) are allowed within the production environment.
A.9.4.5	Access to program source code shall be restricted.	Microsoft enforces access restrictions and supports auditing of the enforcement actions. Access to Microsoft Online Services' source code libraries is limited to authorized Microsoft Online Services Staff and Microsoft Online Services Contractor Staff. Where feasible, source code libraries maintain separate project work spaces for independent projects. Microsoft Online Services Staff and Microsoft Online Services Contractor Staff are granted access only to those work spaces which they need access to perform their duties. An audit log that detailing modifications to the source code library is maintained. Service teams use Active Directory (AD) to control access to change functions. AD is automated, and actions taken (account creation, change, disabling, and removal) are automatically audited.

A.10 CRYPTOGRAPHY

A.10.1 CRYPTOGRAPHIC CONTROLS

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A.10.1.1	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Microsoft develops, documents, and disseminates to all relevant personnel or roles, a system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Encryption mechanisms and techniques used by the service team follow the requirements and restrictions outlined in the Microsoft Security Policy. Service data and information are handled in accordance with the requirements and restrictions specified in the Asset Classification and Protection Standards when cryptography is used. The Asset Classification and Protection Standards establish the mandatory minimum requirements for Microsoft asset ownership, classification, and protection.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		Cryptographic controls are designed and implemented, to protect the confidentiality, integrity and availability of Microsoft Online Services information. Microsoft Online Services provides digital certificates on public facing, external websites. Microsoft Online Services support personnel utilize FIPS 140-2 SSL/TLS encryption for all connections that travel outside the boundary of Microsoft Online Services. SSL/TLS employs cryptographic mechanisms that allow client/server applications to communicate across the network in a way designed to prevent eavesdropping and tampering. Connections within the accreditation boundary occur within Microsoft facilities. Since Microsoft owns and controls access to these connections, they do not require FIPS 140-2 encryption.
A.10.1.2	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Microsoft establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with defined requirements for key generation, distribution, storage, access, and destruction. In accordance with "Public Key Infrastructure Operational Security Standard" which is a component of Microsoft Security Policy, Microsoft Online Services leverages the cryptographic capabilities that are directly a part of the Windows Operating System for certificates and authentication mechanisms (e.g. Kerberos). These cryptographic modules have been certified by NIST as being FIPS 140-2 complaint. Relevant NIST certificate numbers are: 1321, 1333, 1334, 1335, 1336, and 1339. Any time cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data within Microsoft Online Services, the modules and ciphers used are FIPS 140-2 compliant. For additional information on how cryptographic modules are employed in Microsoft products, see TechNet article cc750357: http://technet.microsoft.com/en-us/library/cc750357.aspx

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.11 PHYSICAL AND ENVIRONMENTAL SECURITY		
A.11.1 SECURE AREAS		
Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.		
A.11.1.1	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Microsoft enforces physical access authorizations at defined entry/exit points to the facility where the information system resides by verifying individual access authorizations before granting access to the facility. The exteriors of the data center buildings are non-descript and do not advertise that they are Microsoft data centers. Depending on the design of a data center, physical access authorizations at Microsoft data centers may begin at a controlled perimeter gate or secured facility door that would require either access badge authorization or security officer authorization. Main access to Microsoft data center facilities is restricted to a single point of entry that is manned 24x7 by security personnel. Emergency exits are alarmed and under video surveillance. Electronic access control devices are installed on doors separating the reception area from the facilities' interior to restrict access to approved personnel only. Microsoft data centers have a security operations desk located in the reception area and in line of sight of the single entry point. The data center lobbies have man-trap portal devices that require access card and biometric hand geometry or fingerprint authentication to pass beyond the lobby. Areas within Microsoft data centers that contain critical systems (e.g., co-locations, critical environments, MDF rooms, etc.) are further restricted through various security mechanisms such as electronic access control, biometric devices, and anti-passback controls. Additionally, doors are alarmed and under video surveillance. In addition to the physical entry controls that are installed on various doors within the data center, Microsoft has implemented operational procedures to restrict physical access to authorized employees, contractors and visitors:

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		• Authorization to grant temporary or permanent access to Microsoft data centers is limited to authorized staff. The requests and corresponding authorization decisions are tracked using a ticketing/access system. • Visitors are required to be escorted at all times. The escort's access within the data center is logged and if necessary can be correlated to the visitor for future review. • Badges are issued to personnel requiring access after verification of identification. Microsoft performs a quarterly access list review. As a result of this audit, the appropriate actions are taken after the review.
A.11.1.2	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Microsoft controls physical access to information system distribution and transmission lines within organizational facilities using security safeguards. Microsoft has implemented access control for transmission medium through the design and building of the Main Distribution Frame (MDF) rooms and co-locations to protect information system distribution and transmission lines from accidental damage, disruption, and physical tampering. Access to MDF rooms and colos require two factor authentication (access badge and biometrics). This ensures that access is restricted to only authorized personnel. Within the MDF, transmission and distribution lines are protected from accidental damage, disruption, and physical tampering through the use of metal conduits and locked racks or cages, and cable trays.
A.11.1.3	Physical security for offices, rooms and facilities shall be designed and applied.	Microsoft provides security safeguards to control access to areas within the facility officially designated as publicly accessible. Microsoft data centers utilize physical access devices such as perimeter gates, electronic access badge readers, biometric readers, man-traps/portals, anti-tailgate devices, and anti-pass back controls, as well as security officers to control access to the data centers.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.11.1.4	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Microsoft develops, documents, and disseminates to all relevant personnel or roles procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. The policy is updated annually. Microsoft has implemented the location of information system components control through strategic data center design approach. All Microsoft's Online Services' equipment is placed in locations which have been engineered to be protected from environmental risks such as theft, fire, explosives, smoke, water, dust, vibration, earthquake, harmful chemicals, electrical interference, power outages, electrical disturbances (spikes), and radiation. The facility and infrastructure have implemented seismic bracing for protection against environmental hazards. All of the co-location and MDF rooms are protected by access control, alarms, and video. The facility is also patrolled by security officers 24x7. All portable Microsoft assets are locked or fastened in place in order to provide protection against theft or movement damage.
A.11.1.5	Procedures for working in secure areas shall be designed and applied.	Microsoft develops, documents, and disseminates to all relevant personnel or roles a physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Microsoft has implemented a physical and environmental policy and procedures to allow for the secure operation of Microsoft networks and data centers. The Microsoft Security Policy, Microsoft's Online Services Physical and Environmental Security Standard, Asset Classification Standard, and Asset Protection Standard, are all maintained by Microsoft's Cloud Infrastructure and Operations (MCIO)[1] and reviewed and published annually. These documents address the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide physical and environmental support to Microsoft's online services. The objective of the physical and

[1] MCIO was formerly known as Global Foundation Service (GFS) which is the name referred to in the ISO documentation. Throughout this document, the names MCIO and GFS should be considered synonymous.

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		environmental security policy in the Microsoft Security Policy is to prevent unauthorized access, damage or interference to Microsoft production facilities (data centers). The Microsoft Security Policy applies across the company to all information and processes used in the conduct of Microsoft business. All Microsoft employees and contingent staff are accountable and responsible for complying with these guiding principles within their designated roles. Specific Security Groups (organizations which implement security programs that support this Policy) provide Standards with specific details for the satisfaction of the requirements in this policy. These Standards are followed within the scope of each Security Group's authority. The Microsoft Security Policy constitutes the only Microsoft information security policy. Any exceptions or changes to the policy must be approved by the policy owner. Exceptions or changes to Standards which support this policy must be approved by the applicable Security Group. The Microsoft Security Policy has been reviewed, approved, and is endorsed by Microsoft's senior management. The Microsoft Security Policy is maintained and aligned with supporting corporate policies and functions such as, but not limited to, Human Resources, Legal and Corporate Affairs, and Privacy. Microsoft staff is required to strictly adhere to all applicable security policies, standards, regulations, and requirements.
A.11.1.6	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Microsoft enforces physical access authorizations at entry/exit points to the facility where the information system resides by controlling ingress/egress to the facility using physical access control systems/devices; guards. The exteriors of the data center buildings are non-descript and do not advertise that they are Microsoft data centers. Depending on the design of a data center, physical access authorizations at Microsoft data centers may begin at a controlled perimeter gate or secured facility

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		door that would require either access badge authorization or security officer authorization. Main access to Microsoft data center facilities is restricted to a single point of entry that is manned 24x7 by security personnel. Emergency exits are alarmed and under video surveillance. Electronic access control devices are installed on doors separating the reception area from the facilities' interior to restrict access to approved personnel only. Microsoft data centers have a security operations desk located in the reception area and in line of sight of the single entry point. The data center lobbies have man-trap portal devices that require access card and biometric hand geometry or fingerprint authentication to pass beyond the lobby. Areas within Microsoft data centers that contain critical systems (e.g., co-locations, critical environments, MDF rooms, etc.) are further restricted through various security mechanisms such as electronic access control, biometric devices, and anti-passback controls. Additionally, doors are alarmed and under video surveillance. In addition to the physical entry controls that are installed on various doors within the data center, Microsoft has implemented operational procedures to restrict physical access to authorized employees, contractors and visitors: • Authorization to grant temporary or permanent access to Microsoft data centers is limited to authorized staff. The requests and corresponding authorization decisions are tracked using a ticketing/access system. • Visitors are required to be escorted at all times. The escort's access within the data center is logged and if necessary can be correlated to the visitor for future review. • Badges are issued to personnel requiring access after verification of identification. Microsoft performs a quarterly access list review. As a result of this audit, the appropriate actions are taken after the review.
A.11.2 EQUIPMENT		
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.		

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.11.2.1	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Microsoft positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. Microsoft has implemented the location of information system components control through strategic data center design approach. All Microsoft's online services' equipment is placed in locations which have been engineered to be protected from environmental risks such as theft, fire, explosives, smoke, water, dust, vibration, earthquake, harmful chemicals, electrical interference, power outages, electrical disturbances (spikes), and radiation. The facility and infrastructure have implemented seismic bracing for protection against environmental hazards. All of the co-location and MDF rooms are protected by access control, alarms, and video. The facility is also patrolled by security officers 24x7. All portable Microsoft assets are locked or fastened in place in order to provide protection against theft or movement damage.
A.11.2.2	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Microsoft protects power equipment and power cabling for the information system from damage and destruction. Microsoft data centers have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, i.e. generators. Regular maintenance and testing is conducted for both the UPS and generators. Data centers have made arrangements for emergency fuel delivery. Power systems also utilize redundancy as form of protection. Data centers utilize multiple power/utility feeds into the facility as well as redundant configurations of generators and UPS systems. Generator and UPS system components undergo regular maintenance procedures to maintain the systems in proper working order. Cables, electrical lines, and backup generators—must be placed in environments which have been engineered to be protected from environmental risks such as theft, fire, explosives, smoke, water, dust, vibration, earthquake, harmful chemicals, electrical interference, power outages, electrical disturbances (spikes). The data center has a dedicated Facility Operations Center to monitor the following:

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		• Power systems, including all critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment. • The Heating, Ventilation and Air Conditioning (HVAC) system, which controls and monitors space temperature and humidity within the data centers, space pressurization and outside air intake. Fire Detection and Suppression systems exist at all data centers. Additionally, portable fire extinguishers are available at various locations in the data center. Routine maintenance is performed on facility and environmental protection equipment.
A.11.2.3	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Microsoft protects power equipment and power cabling for the information system from damage and destruction. Microsoft has implemented access control for transmission medium through the design and building of the Main Distribution Frame (MDF) rooms and co-locations to protect information system distribution and transmission lines from accidental damage, disruption, and physical tampering. Access to MDF rooms and colos require two factor authentication (access badge and biometrics). Microsoft has implemented the protection of power equipment and power cabling by providing protective spaces and appropriate labeling for cables. Microsoft infrastructure equipment—for example, cables, electrical lines, and backup generators—must be placed in environments which have been engineered to be protected from environmental risks such as theft, fire, explosives, smoke, water, dust, vibration, earthquake, harmful chemicals, electrical interference, power outages, electrical disturbances (spikes), and radiation. Power and information system cables within any Microsoft data center environment are labeled appropriately and protected against interception or damage. Power and information system cables are separated from each other at all points within an environment to avoid interference. All electrical spaces are behind card readers or additional key locks as appropriate. Access hallways as well as exterior entrances and equipment yards approaching the

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		protective spaces are all monitored via video surveillance. Power systems also utilize redundancy as form of protection. Data centers utilize multiple power/utility feeds into the facility as well as redundant configurations of generators and UPS systems. Generator and UPS system components undergo regular maintenance procedures to maintain the systems in proper working order.
A.11.2.4	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Microsoft schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The Critical Environment (CE) team schedules, performs, documents, and reviews all maintenance activities performed on CE components. Microsoft data centers rely on a computerized maintenance management system (CMMS) to manage maintenance schedules and work order management. Work orders are generated based on OEM guidelines and assigned for completion. All maintenance work performed at a Microsoft data center must follow approved instructions captured in a Method of Procedure (MOP) document. A MOP must have data center management approval before work can begin. Completed MOPs are reviewed and receive data center management sign-off to indicate completion. Details of completed MOPs are stored in CMMS and then the work order closed.
A.11.2.5	Equipment, information or software shall not be taken off-site without prior authorization.	Microsoft approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. DC Management is responsible for all CE maintenance that is performed either onsite or remotely. Data Center Management generally consists of Microsoft full time employees who serve in the following roles: Data Center Manager (DCM), Facilities Program Manager (FPM), and Technical Program Manager (TPM). The FPM and DCM are responsible for work occurring in the DC critical environment. CE maintenance is prescribed in required step by step documents called Methods of Procedure (MOP). MOPs are reviewed/approved by data center management prior to any work beginning. MOPs serve

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		as the checklist for the maintenance procedure and the documentation of the work completed. CE maintenance is performed in areas of the data center that are controlled and protected by physical security mechanisms (e.g. approved access, cameras, 2FA: access badges, biometrics, security patrols).
A.11.2.6	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Microsoft implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. The use and/or storage of Microsoft managed information processing equipment and/or media containing HBI or MBI data (as defined by the Microsoft policy) outside a Microsoft Online Services managed facility must be approved by the asset owner(s). Protection afforded to equipment and/or media located outside a Microsoft Online Services managed facility is commensurate with protection afforded to equipment and media located in a Microsoft Online Services managed facility.
A.11.2.7	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Microsoft employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. Microsoft uses data erasure units and processes to cleanse/purge data in a manner consistent with NIST SP 800-88 and which are commensurate with the Microsoft asset classification of the asset. For assets requiring destruction, Microsoft utilizes onsite asset destruction services.
A.11.2.8	Users shall ensure that unattended equipment has appropriate protection.	Microsoft prevents access to the system by initiating a session lock after a period of inactivity or upon receiving a request from a user. Microsoft Online Services has policies that define session time-out requirements.
A.11.2.9	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Microsoft physically controls and securely stores digital and/or non-digital media controlled areas. Microsoft has implemented media protection policy through the publication of the Microsoft Security Policy. The Microsoft Security Policy describes how important organizational records relating to the organization's Information Security Program, independent of media type, must be retained, stored, protected, and, if

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		appropriate, destroyed according to the established information handling procedures for the records. Such records must be retained in controlled facilities for protection against loss, destruction, and falsification. In addition, measures must be put in place to ensure the ability to recover these records into a useable format for the duration of the records’ retention period. The Asset Classification Standard and Asset Protection Standard define appropriate handling and protection mechanisms of assets based on their classification. The Microsoft Security Policy is reviewed, updated, and approved annually. The Microsoft Security Policy applies across the company to all information and processes used in the conduct of Microsoft business. All Microsoft employees and contingent staff are accountable and responsible for complying with these guiding principles within their designated roles. The Asset Classification Standard and Asset Protection Standard addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to Microsoft’s online services for media protection. Microsoft’s Online Services Asset Classification and Protection Standards demonstrate a high level of management commitment and are a component of the MCIO Risk Management Program strategy. This document provides online services staff with a current set of clear and concise information security requirements as they pertain to media protection. The Asset Classification Standard and Asset Protection Standard are reviewed annually by the management teams of online properties adhering to Microsoft Security Policy. This satisfies media protection policy and procedure through effective management and monitoring of risks associated with this control.

A.12 OPERATIONS SECURITY

A.12.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES

Objective: To ensure correct and secure operations of information processing facilities.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.12.1.1	Operating procedures shall be documented and made available to all users who need them.	Microsoft develops, documents, and disseminates to all users a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The Microsoft Security Policy contains rules and requirements that must be met in the delivery and operation of Microsoft Online Services. More detailed requirements are established within Microsoft Security Procedures and service team-specific standard operating procedures (SOPs). These standards and procedures act as adjuncts to the security policy and provide implementation level details to carry out specific operational tasks.
A.12.1.2	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Microsoft implements approved configuration-controlled changes to the information system. An operational change control procedure is in place for Microsoft Online Services and system changes. This procedure includes a process for Microsoft Online Services management review and approval. This change control procedure is communicated to all parties (Microsoft Online Services and third parties) who perform system maintenance on, or in, any of the Microsoft Online Services facilities. The operational change control procedure considers the following actions: • The identification and documentation of the planned change • An assessment process of possible change impact • Change testing in an approved non-production environment • Change communication plan • Change management approval process • Change abort and recovery plan (when applicable)
A.12.1.3	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	Microsoft conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. Microsoft proactively monitors and continuously measures the performance of key subsystems of the Microsoft Online Services platform against the established boundaries for acceptable service

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		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. System performance and capacity utilization is proactively planned to optimize the environment. The proactive capacity management is based on defined thresholds or events; hardware and software subsystem monitoring for acceptable service performance and availability, CPU utilization, service utilization, storage utilization and network latency.
A.12.1.4	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Microsoft analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. Microsoft Online Services systems are partitioned at multiple layers to support system confidentiality, integrity and availability. These partitions can be divided into two categories: physical partitions and logical partitions. Microsoft Online Services systems are also housed in datacenters under strong physical protections. Physical access is restricted to Data Center personnel only, and governed by least privilege. Additionally, logical partitions provide a layered defense for Microsoft Online Services systems. The preferred method for logically partitioning systems, at the network level, are router ACLs, VLANs, and appropriately placed firewalls. Microsoft operates both types of devices for Microsoft Online Services properties. This partitioning strategy is used to separate front end components (e.g. web servers) from the back end components (e.g. databases or management devices) of each system. Microsoft Online Services production environments are logically partitioned from all other environments (e.g. various development environments) in the same manner.
A.12.2 PROTECTION FROM MALWARE		
Objective: To ensure that information and information processing facilities are protected against malware.		
A.12.2.1	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Microsoft implements controls for detection, prevention, and recovery against malware. The use of anti-virus software is a principal mechanism for protection of Microsoft Online Services assets from

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		malicious software. The software will detect and prevent the introduction of computer viruses and worms onto the service systems. The software will also quarantine infected systems, and prevent further damage until remediation steps are taken. Anti-virus software provides both preventive and detective control over malicious software. Forefront Endpoint Protection (FEP) or Symantec EndPoint Protection (SEP) is installed as part of the initial build on all systems. Additionally, SPO utilized Forefront for SharePoint enabling further protection by actively scanning document repositories and code within the SharePoint sites and libraries. Once the appropriate AV tool is installed, the following functions will be centrally managed: • Periodic scans of the file system • Automatic scans of the environment • Testing, identification, and rectification of false positives generated by the tool Microsoft Online Services is an isolated server centric environment which mobile code (software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction i.e. ActiveX, Java Script) isn't as applicable as in a desktop environment. In addition, all mobile code in use in the environment is developed or reviewed by the service team. All releases have release-specific implementation guidance and testing to ensure that only acceptable code is released. Antivirus tools scan mobile code when that code is loaded onto each server. Additional mobile code protection is a function of the application in most cases.
A.12.3 BACKUP		
Objective: To protect against loss of data.		
A.12.3.1	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Microsoft regularly tests backup information to verify media reliability and information integrity. Microsoft Online Services systems do not use any media backups. Microsoft Online Services utilize Data Center replication solutions. Each of the Microsoft Online Services systems' Business Continuity Plans indicates the procedures in place for the replication of Microsoft Online Services data.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.12.4 LOGGING AND MONITORING		
Objective: To record events and generate evidence.		
A.12.4.1	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Microsoft regularly reviews and updates the list of auditable events. Microsoft Online Services has in-service logs and compliance features that enable customers to directly view a subset of logs to verify who's accessed what data, and what they did with it. This includes viewing mailbox usage, administration activities and SharePoint sites. In-service features that provide this visibility include Exchange Auditing, SharePoint Auditing, the Discovery Center console, and the administrator portal. Please review the Reports section of the Office 365 Service Description for more detail. The Microsoft Online Services Security Service Engineering team has developed a general set of auditable events specific to the Microsoft Online Services based on ongoing risk assessments of the system which incorporate identified vulnerabilities, business requirements, and Microsoft Security Standards. The general event set is reviewed by Security Service Engineering when a significant change to the system is made to ensure any vulnerabilities exposed are being addressed by the set of auditable events. New events may be incorporated when a new service is brought online or when a vulnerability or threat is identified (e.g. - through security assessments, security bulletins, etc.). When changes to the Microsoft Online Services need to be made, they are executed through Microsoft Online Services Change Management. The change management process also includes a risk assessment of the change.
A.12.4.2	Logging facilities and log information shall be protected against tampering and unauthorized access.	Microsoft protects facilities and log information against tampering and unauthorized access. Audit records are continually analyzed for indications of inappropriate or unusual activity using a formal monitoring process. Findings are reported using the security incident response process. Microsoft Online Services has formal monitoring processes to include frequency of review for Standard

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		Operating Procedures and review oversight processes and procedures. Microsoft's presumed breach stance involves auditing all operator/administrator access and actions.
A.12.4.3	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Microsoft protects audit information and audit tools from unauthorized access, modification, and deletion. Microsoft's presumed breach philosophy involves auditing all operator/administrator access and actions. The Microsoft Online Services Security Service Engineering team has developed a general set of auditable events specific to the Microsoft Online Services Support based on ongoing risk assessments of the system which incorporate identified vulnerabilities, business requirements, and Microsoft Online Services Security Standards. The general event set is reviewed by Security Service Engineering when a significant change to the system is made to ensure any vulnerabilities exposed are being addressed by the set of auditable events. New events may be incorporated when a new service is brought online or when a vulnerability or threat is identified (e.g. - through security assessments, security bulletins, etc.). When changes to the Microsoft Online Services need to be made, they are executed through Microsoft Online Services Change Management. The change management process also includes a risk assessment of the change.
A.12.4.4	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	Microsoft records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Audit records and events generated by Microsoft Online Services are logged with timestamps, which are recorded from the internal Windows Time service. All servers are configured to synchronize internal clocks with environment domain controllers via NTP. All servers are joined to an Active Directory domain and configured to receive authenticated time updates from the local domain controller via NTP and synchronize at least hourly. Domain Controllers sync to the Primary Domain Controller, which is located in the US.

A.12.5 CONTROL OF OPERATIONAL SOFTWARE

Objective: To ensure the integrity of operational systems.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.12.5.1	Procedures shall be implemented to control the installation of software on operational systems.	Microsoft develops, documents, and disseminates to all relevant personnel or roles, procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. Patches, updates and threat mitigation are all covered by the Microsoft Security Development Lifecycle (SDL). Part of the SDL has been built upon investments in Microsoft Trustworthy Computing. We have various patch management release cycles and engagement models that allow us to mitigate new threats as quickly as possible within the service. As established by the Microsoft Security Policy, the following guidelines are in place regarding the installation of software within the Microsoft Online Services environment: • All software (including tools and utilities) installed within the Microsoft Online Services environment must be approved by the appropriate stakeholders prior to being released into production. • Prior to deployment in any Microsoft Online Services operated environment, all software must be tested in a manner suitable to Microsoft to evaluate its impact on system performance, stability (failure and recovery characteristics) and security state (security controls work as expected and the product does not contain malicious code). • Software submitted for approval must have a legitimate business purpose. Additionally, all installation of software in Microsoft Online Services environments is governed by access controls.
A.12.6 TECHNICAL VULNERABILITY MANAGEMENT		
Objective: To prevent exploitation of technical vulnerabilities.		
A.12.6.1	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Microsoft identifies, reports, and corrects information system flaws. Microsoft Online Services identifies, reports, and corrects information system flaws through vulnerability management, incident response management, and patch / configuration management processes. The Microsoft Online Services Security Incident Response Program assists with identifying and reporting of information system flaws. Microsoft Online Services receives vulnerability-related data from multiple sources of information which

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		include: Microsoft Security Resource Center (MSRC), vendor Web sites, other third-party services (e.g., Internet Security Systems) and internal / external vulnerability scanning of services. Microsoft Online Services Security Service Engineering will determine which updates are applicable within the Microsoft Online Services environment. Potential changes are tested in advance. Patching schedules are defined by Microsoft Online Services Security Service Engineering as follows: • 30 days for high vulnerabilities • 90 days for medium/moderate vulnerabilities Microsoft works with a variety of different industry bodies and security experts to understand new threats and evolving trends. We constantly scan our systems for vulnerabilities and we contract with external penetration testers who also constantly scan the systems.
A.12.6.2	Rules governing the installation of software by users shall be established and implemented.	Microsoft establishes policies governing the installation of software by users. The Microsoft Online Services Acceptable Use Standard details acceptable and unacceptable use of Microsoft Online Services IT assets, including the use of elevated privileges and communications software. The Microsoft Online Services Acceptable Use Standards is a component of the Microsoft Online Services Information Security Policy. The Policy has been reviewed, approved, and is endorsed by Microsoft Online Services management. The purpose of this policy is to outline Microsoft Online Services security principles and to supplement Microsoft's acceptable use standard with Microsoft Online Services specific acceptable usage standard of Microsoft Online Services technology assets. This document details acceptable and unacceptable use of Microsoft Online Services IT organization, including the use of elevated privileges and communications software. It is the responsibility of all Microsoft Online Services staff to read and understand this policy and the Microsoft Online Services Security Policy. All Microsoft

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		Online Services staff must indicate they have reviewed, and agree to adhere to, all policies within the Microsoft Online Services Security Documentation per the methods indicated in the Microsoft Online Services Security Policy. Any Microsoft Online Services staff that does not follow Microsoft Online Services policies may be subject to disciplinary action, up to and including immediate termination.
A.12.7 INFORMATION SYSTEMS AUDIT CONSIDERATIONS		
Objective: To minimize the impact of audit activities on operational systems.		
A.12.7.1	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	Microsoft regularly reviews and updates the current audit and accountability policy. A scope and approach is detailed as part of the compliance planning phase for both internal and external independent audits which identifies those controls that will be tested, the tools and techniques that will be used, required access or privilege of audit software and service personnel support/hours required. Coordination with the service/asset owners and management is conducted to communicate compliance assessment or audit plans, identify potential project risks, verify available service personnel support and identify risks to services and strategies posed by assessments/audits. Plans are agreed to mitigate risk to services that still enable compliance assessment objectives to be achieved in a timely manner.
A.13 COMMUNICATIONS SECURITY		
A.13.1 NETWORK SECURITY MANAGEMENT		
Objective: To ensure the protection of information in networks and its supporting information processing facilities.		
A.13.1.1	Networks shall be managed and controlled to protect information in systems and applications.	Microsoft protects the confidentiality and integrity of transmitted information. To maintain the confidentiality and integrity of customer data, Microsoft keeps consumer services networks separate from Microsoft Online Services networks. Multiple techniques are used to control information flows, including but not limited to: • Physical separation. Network segments are physically separated by routers that are

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		configured to prevent specific communication patterns. • Logical separation. Virtual LAN (VLAN) technology is used to further separate communications. • Firewalls. Firewalls and other network security enforcement points are used to limit data exchanges with systems that are exposed to the Internet, and to isolate systems from back-end systems managed by Microsoft. • Protocol restrictions • All traffic to and from customers are transmitted over encrypted connections. Microsoft Online Services implements boundary protection through the use of controlled devices at the network boundary and at key points within the network. The overarching principle of network security is to allow only connection and communication that is necessary to allow systems to operate, blocking all other ports, protocols and connections by default. Access Control Lists (ACLs) are the preferred mechanism through which to restrict network communications by source and destination networks, protocols, and port numbers. Approved mechanisms to implement networked-based ACLs include: Tiered ACLs on routers managed by MCIO, IPSec policies applied to hosts to restrict communications (when used in conjunction with tiered ACLs), firewall rules, and host-based firewall rules. Microsoft Online Services implements information flow control by allowing only connections and communication which are necessary to allow systems to operate, blocking all other ports, protocols and connections by default, as defined in Microsoft's Online Services Security Standard. Access Control Lists (ACLs) are the preferred mechanism to restrict network communications by source and destination networks, protocols, and port numbers. Microsoft Online Services manages ACL approvals through the RFC process (including review and risk acceptance) and the change process, and MCIO implements the approved change. Approved mechanisms to implement networked-based ACLs include: ACLs on routers managed by MCIO and firewall rules.

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		Microsoft provides FIPS 140-2 cipher support for customer, third party, and remote access connections into the FISMA accreditation boundary. Microsoft Online Services support personnel utilize FIPS 140-2 SSL/TLS encryption for all connections that travel outside the boundary of Microsoft Online Services. SSL/TLS employs cryptographic mechanisms that allow client/server applications to communicate across the network in a way designed to prevent eavesdropping and tampering. Connections within the accreditation boundary occur within MCIO facilities. Since MCIO owns and controls access to these connections, they do not require FIPS 140-2 encryption.
A.13.1.2	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Microsoft authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements. Microsoft requires all third parties (external information system services) who are engaged with Microsoft Online Services to sign a Microsoft Master Vendor Agreement (MMVA). The MMVA requires the third party to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of Microsoft confidential information. Microsoft includes provisions in the MMVA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Vendors that handle sensitive data must be in compliance with Microsoft vendor privacy practices and data protection requirements.
A.13.1.3	Groups of information services, users, and information systems shall be segregated on networks.	Microsoft separates user functionality (including user interface services) from information system management functionality. The overarching principle of network security is to allow only connection and communication that is necessary to allow systems to operate, blocking all other ports, protocols and connections by default. The networks within the Microsoft Online Services data centers are designed to create multiple separate network segments. This segmentation helps to provide physical separation of critical, back-end servers and storage devices from the public-facing interfaces. Data storage and processing is logically segregated among customers of the same service through Active Directory® structure and capabilities specifically

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		developed to help build, manage, and secure multitenant environments. The multitenant security architecture ensures that customer data stored in shared Microsoft Online Services data centers is not accessible by or compromised to any other organization. Organizational Units (OUs) in Active Directory control and prevent the unauthorized and unintended information transfer via shared system resources. Tenants are isolated from one another based on custom code and security boundaries, or silos, enforced logically through Active Directory.
A.13.2 INFORMATION TRANSFER		
Objective: To maintain the security of information transferred within an organization and with any external entity.		
A.13.2.1	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Microsoft develops, documents, and disseminates to all relevant personnel and roles procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. The Microsoft Security Policy defines Microsoft Online Services policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Microsoft Online Services. The Microsoft Security Policy contains rules and requirements that must be met in the delivery and operation of Microsoft Online Services. Policies and procedures are distributed to personnel with responsibilities for implementing those policies and procedures via email links to SharePoint. Microsoft Online Services implements boundary protection through the use of controlled devices at the network boundary and at key points within the network. The overarching principle of network security is to allow only connection and communication that is necessary to allow systems to operate, blocking all other ports, protocols and connections by default. Access Control Lists (ACLs) are the preferred mechanism through which to restrict network communications by source and destination networks, protocols, and port numbers. Approved mechanisms to implement networked-based ACLs include: Tiered ACLs on routers managed by MCIO, IPSec policies applied to hosts to restrict

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		communications (when used in conjunction with tiered ACLs), firewall rules, and host-based firewall rules. Microsoft provides FIPS 140-2 cipher support for customer, third party, and remote access connections into the FISMA accreditation boundary. Microsoft Online Services support personnel utilize FIPS 140-2 SSL/TLS encryption for all connections that travel outside the boundary of Microsoft Online Services. SSL/TLS employs cryptographic mechanisms that allow client/server applications to communicate across the network in a way designed to prevent eavesdropping and tampering. Connections within the accreditation boundary occur within MCIO facilities. Since MCIO owns and controls access to these connections, they do not require FIPS 140-2 encryption.
A.13.2.2	Agreements shall address the secure transfer of business information between the organization and external parties.	Microsoft documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated. This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. Microsoft requires all third parties (external information system services) who are engaged with Microsoft Online Services to sign a Microsoft Master Vendor Agreement (MMVA). The MMVA requires the third party to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of Microsoft confidential information. Microsoft includes provisions in the MMVA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Vendors that handle sensitive data must be in compliance with Microsoft vendor privacy practices and data protection requirements.
A.13.2.3	Information involved in electronic messaging shall be appropriately protected.	Microsoft maintains the confidentiality and integrity of information during preparation for transmission and during reception. Procedures for the handling of Assets in all forms are in accordance with the relevant standards and procedures. These standards are met throughout the existence of the Asset, from acquisition, during storage, during transmission, and through disposal.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.13.2.4	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Microsoft ensures that access to classified information requiring special protection is granted only to individuals who have read, understood, and signed a nondisclosure agreement. The Microsoft Online Services Acceptable Use Policy outlines the Online Services specific acceptable usage standards of the Infrastructure & Services technology assets. Additionally, the Microsoft General Use Standard describes user responsibilities and establishes expected behavior when using Microsoft Online Services and other Microsoft systems. All users, including employees, vendors, and contractors are required to follow the rules of behavior, which are outlined in the Microsoft General Use Standard. The agreements are put in place to protect trade secrets, sensitive, or business confidential information and assets. The NDA, Employee Handbook, and Microsoft Security Policy include statements regarding information and asset protection responsibilities. They also describe the penalties for the violation of these responsibilities. Microsoft Human Resources reviews these agreements monthly.

A.14 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

A.14.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle.

This also includes the requirements for information systems which provide services over public networks.

A.14.1.1	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Microsoft develops an information security architecture for the information system that describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information. Microsoft's implementation of life cycle support is outlined through Microsoft Security Development Lifecycle (SDL), (SDL) process that is followed by all engineering and development projects. A security requirements analysis must be completed for all system development projects. This analysis document acts as a framework and includes the identification of possible risks to the finished development project as well as mitigation strategies which can be implemented and tested during the development phases. Critical security

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		review and approval checkpoints are included during the system development life cycle. All members of software development teams receive appropriate training to stay informed about security basics. Microsoft Online Services implements the acquisitions control through enforcement of the Microsoft Security Policy. The Policy dictates that where a third party is allowed to (i) access, process, host or manage Microsoft's online services' information assets or information processing facilities, or (ii) add products or services to Microsoft's online services' information processing facilities, arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved. Appropriate security standards are addressed in the agreement, to provide a level of protection.
A.14.1.2	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Microsoft implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by alternative physical safeguards. Microsoft Online Services implements boundary protection through the use of controlled devices at the network boundary and at key points within the network. The overarching principle of network security is to allow only connection and communication that is necessary to allow systems to operate, blocking all other ports, protocols and connections by default. Access Control Lists (ACLs) are the preferred mechanism through which to restrict network communications by source and destination networks, protocols, and port numbers. Approved mechanisms to implement networked-based ACLs include: Tiered ACLs on routers managed by MCIO, IPSec policies applied to hosts to restrict communications (when used in conjunction with tiered ACLs), firewall rules, and host-based firewall rules. Approved mechanisms to implement networked-based ACLs include: ACLs on routers managed by MCIO, IPSec policies applied to hosts to restrict communications (when used in conjunction with ACLs), firewall rules, and host-based firewall rules.

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		Microsoft Online Services service teams also implement encryption mechanisms on all communications between partners and between customers. For example, Exchange must authenticate using SSL to WAC when requesting a document for rendering. All encryption modules are operated in FIPS mode which has been FIPS 140-2 certified. This ensures the confidentiality and integrity of communications between services teams, partners, and customers are protected. Microsoft provides FIPS 140-2 cipher support for customer, third party, and remote access connections into the FISMA accreditation boundary. Microsoft Online Services support personnel utilize FIPS 140-2 SSL/TLS encryption for all connections that travel outside the boundary of Microsoft Online Services. SSL/TLS employs cryptographic mechanisms that allow client/server applications to communicate across the network in a way designed to prevent eavesdropping and tampering. Microsoft Online Service's FIPS 140-2 encryption modules used for transmitted information are certified by NIST via certificates 1334, 1335, and 1336. Connections within the accreditation boundary occur within MCIO facilities. Since MCIO owns and controls access to these connections, they do not require FIPS 140-2 encryption. The initial login page of Microsoft Online Services is publicly accessible as well as the OnRamp login page. Integrity and availability of this information is protected equivalently to all other Microsoft Online Services information. Any changes made to this information passes through normal change control processes. Microsoft Online Services DNS provides DNS resolution services for Microsoft Online Services URLs. This must be publicly available per the technical specification of DNS and for the service to operate. Microsoft Online Services DNS only exposes the registered DNS ports to the public internet (TCP/UDP 53) through MCIO can only be modified via the web service exposed to partners. All requests to the web service must be authenticated and are encrypted through the use of SSL certificates. This protects the integrity of DNS information by ensuring only authorized services can write to the DNS database.

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
A.14.1.3	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Microsoft implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by alternative physical safeguards. Microsoft support personnel utilize FIPS 140-2 SSL/TLS encryption for all connections that travel outside the boundary of Microsoft Online Services. SSL/TLS employs cryptographic mechanisms that allow client/server applications to communicate across the network in a way designed to prevent eavesdropping and tampering. Microsoft Online Service's FIPS 140-2 encryption modules used for transmitted information are certified by NIST via certificates 1334, 1335, and 1336. Connections within the accreditation boundary occur within MCIO facilities. Since MCIO owns and controls access to these connections, they do not require FIPS 140-2 encryption.

A.14.2 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

A.14.2.1	Rules for the development of software and systems should be established and applied to developments within the organization.	Microsoft manages the information system using a system development life cycle that incorporates information security considerations. Microsoft's implementation of life cycle support is outlined through Microsoft's Security Development Lifecycle (SDL) process that is followed by all engineering and development projects. This is a software development model that includes specific security considerations. A security requirements analysis must be completed for all system development projects. This analysis document acts as a framework and includes the identification of possible risks to the finished development project as well as mitigation strategies which can be implemented and tested during the development phases. Critical security review and approval checkpoints are included during the system development life cycle. All members of software development teams receive appropriate training to stay informed about security basics and recent trends in security and privacy. Individuals who develop software programs are required to attend at least one security training class each year. Security training helps ensure software is created with

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		security and privacy in mind and also helps development teams stay current on security issues. Project team members are strongly encouraged to seek additional security and privacy education that is appropriate to their needs or products. The Microsoft SDL process includes the following phases: • Phase 1: Requirements - The Requirements phase of the SDL includes the project inception—when the organization considers security and privacy at a foundational level—and a cost analysis—when determining if development and support costs for improving security and privacy are consistent with business needs. This phase also includes defining security roles and responsibilities and identifying individuals with these roles and responsibilities. • Phase 2: Design - The Design phase is when the organization builds the plan for how to take the project through the rest of the SDL process—from implementation, to verification, to release. During the Design phase the organization establishes best practices to follow for this phase by way of functional and design specifications, and by performing risk analysis to identify threats and vulnerabilities in the software. TMA (Threat Model Analysis) is required to define all attack surfaces and their associated risks; all security gaps and risks and documented and analyzed. This security impact analysis will result in dataflow documentation in order to identify all intended paths for information and potential attack vectors. • Phase 3: Implementation - The Implementation phase is when the organization creates the documentation and tools the customer uses to make informed decisions about how to deploy the software securely. To this end, the Implementation phase is when the organization establishes development best practices to detect and remove security and privacy issues early in the development cycle. Initial testing of elements begins in this phase • Phase 4: Verification - During the Verification phase, the organization ensures that the code meets the security and privacy tenets established in the previous phases. This is done through security and privacy testing, and a security push—which is a team-wide focus

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		on threat model updates, code review, testing, and thorough documentation review and edit. Additionally, service teams create a Security Incident Response document as part of their SDL requirements that outlines how security-specific incidents are addressed. A public release privacy review is also completed during the Verification phase. • Phase 5: Release - The Release phase is when the organization prepares the software for consumption and prepares for what happens once the software is released. One of the core concepts in the Release phase is response planning—mapping out a plan of action, should any security or privacy vulnerabilities be discovered in the release—and this carries over to post-release, as well, in terms of response execution. To this end, a Final Security Review and privacy review is required prior to release. After a software program is released, the product development team must be available to respond to any possible security vulnerabilities or privacy issues that warrant a response. In addition, the development team is required to create a response plan that includes preparations for potential post-release issues. Microsoft Online Services has implemented information validation through checking of data inputs as part of the SDL process. Thorough code reviews and testing are completed during the Verification Phase of the SDL prior to software being put into a production environment. The code reviews and testing check for cases of SQL injection, format string vulnerabilities, XSS, integer arithmetic, command injection, and buffer overflow vulnerabilities. This satisfies the life cycle support control through effective management of the risks associated with failing to implement a system development life cycle methodology that lacks information security considerations. The following software is used in the implementation of the SDL: • SDL Threat Modeling Tool: This tool helps developers analyze possible security issues. • FxCop for SDL: FxCop assesses system software for consistency with code rules required by the SDL.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		• Attack Surface Analyzer: This tool helps developers detect application and host level attack surfaces. • BinScope: This tool analyzes software binaries for possible security issues. • PREFast: This is a static code security analysis tool. • FileFuzzer: This tool modifies system inputs dynamically to test for security weaknesses. • Prefix: This tool assesses code for security issues during compilation. For more details on the SDL process, please refer to http://www.microsoft.com/security/sdl/
A.14.2.2	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Microsoft determines the types of changes to the information system that are configuration controlled. A formal change control procedure is followed when making changes to any production Microsoft Online Services system. This procedure includes a review and approval process. This change control procedure is communicated to all Microsoft Online Services Staff with a need to know and Microsoft Online Services Contractor Staff with a need to know and third parties who perform system maintenance on, or in, any of the Microsoft Online Services facilities. At a minimum, the procedure includes the following actions: • The identification and documentation of the planned change • Assessment of the change impact • Change testing in an appropriate non-production environment • Change Communication plan • Change management approval process • Change abort and recovery plan A centralized change management tool is used to document evidence of approval and track all changes.
A.14.2.3	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Microsoft tests, validates, and documents changes to the information system before implementing the changes on the operational system. The service team follows the SDL process, which involves testing within a segregated environment, code review and documentation of changes within change management tool. Technical reviews of significant Microsoft Online Services system changes are performed and approved by Change Advisory Boards.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.14.2.4	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.	Microsoft determines the types of changes to the information system that are configuration controlled. Microsoft Online Services has implemented the configuration management policy and procedures control through the Microsoft Security Policy. Changes to operational systems, other than security patches, can only be made when there is a valid business reason to do so, such as a planned upgrade to the system. Changes implemented within the production environment are categorized into RFC types to appropriately schedule, align resources, and provide change metrics back into the change process for continuous improvement. Security impact analysis considers the configurable security-related parameters of Microsoft Online Services such as registry settings, account, file, and directory settings (i.e., permissions), and settings for services, ports, protocols, and remote connections. Security Impact Analysis is performed for all the new features and code changes. Modifications to software packages are not made unless explicitly approved by the Microsoft Online Services management and version and change control procedures have occurred.
A.14.02.5	Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.	Microsoft applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. The Microsoft SDL process is followed for all engineering and development projects. The Microsoft SDL process includes the following phases which implement standard security engineering principles across all Microsoft Online Services systems: • Phase 1: Requirements - The Requirements phase of the SDL includes the project inception—when the organization considers security and privacy at a foundational level—and a cost analysis—when determining if development and support costs for improving security and privacy are consistent with business needs. • Phase 2: Design - The Design phase is when the organization builds the plan for how to take the project through the rest of the SDL process—from implementation, to verification, to release. During the

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		Design phase the organization establishes best practices to follow for this phase by way of functional and design specifications, and by performing risk analysis to identify threats and vulnerabilities in the software. • Phase 3: Implementation - The Implementation phase is when the organization creates the documentation and tools the customer uses to make informed decisions about how to deploy the software securely. To this end, the Implementation phase is when the organization establishes development best practices to detect and remove security and privacy issues early in the development cycle. • Phase 4: Verification - During the Verification phase, the organization ensures that the code meets the security and privacy tenets established in the previous phases. This is done through security and privacy testing, and a security push—which is a team-wide focus on threat model updates, code review, testing, and thorough documentation review and edit. A public release privacy review is also completed during the Verification phase. • Phase 5: Release - The Release phase is when the organization prepares the software for consumption and prepares for what happens once the software is released. One of the core concepts in the Release phase is response planning—mapping out a plan of action, should any security or privacy vulnerabilities be discovered in the release—and this carries over to post-release, as well, in terms of response execution. To this end, a Final Security Review and privacy review is required prior to release. As established by the Microsoft Online Services Security Policy application code changes must be reviewed and approved by the Microsoft Online Services Security Team. Additionally, the security requirements of the system are reviewed on an annual basis. SDL Track is the online tool used to monitor the progress of all engineering initiatives and controls the process to ensure that all steps are followed. The System Owner is responsible for ensuring that the SDL process is followed for all engineering initiatives associated with Microsoft Online Services.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.14.02.6	Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Microsoft integrates the organizational information security risk management process into system development life cycle activities. Microsoft's implementation of life cycle support is outlined through Microsoft Security Development Lifecycle (SDL), (SDL) process that is followed by all engineering and development projects. A security requirements analysis must be completed for all system development projects. This analysis document acts as a framework and includes the identification of possible risks to the finished development project as well as mitigation strategies which can be implemented and tested during the development phases. Critical security review and approval checkpoints are included during the system development life cycle. All members of software development teams receive appropriate training to stay informed about security basics.
A.14.2.7	The organization shall supervise and monitor the activity of outsourced system development.	Microsoft employs processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. The Microsoft Master Vendor Agreement (MMVA) requires the third party to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of Microsoft confidential information. Microsoft includes provisions in the MMVA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Vendors that handle sensitive data must be in compliance with Microsoft vendor privacy practices and data protection requirements.
A.14.02.08	Testing of security functionality should be carried out during development.	Microsoft requires the developer of the production, system component, or production service to perform testing/evaluation during development. The service team is responsible for ensuring that all system development and maintenance activities are performed in accordance with the Microsoft SDL process. A formal review process is implemented to ensure that new or modified source code authored by Microsoft's online services staff is developed in a secure fashion, no malicious code has been introduced into the system,

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		and that proper coding practices are followed. The reviewers' names, review dates, and review results are documented and maintained for audit purposes. A formal security quality assurance process is implemented to test for vulnerabilities to known security exposures and exploits. The process includes the use of automated security testing tools and requires that all high vulnerabilities get remediated before the system will be released to production.
A.14.2.9	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Microsoft requires the developer of the production, system component, or production service to perform testing/evaluation during development. The service team is responsible for ensuring that all system development and maintenance activities are performed in accordance with the Microsoft SDL process. A formal review process is implemented to ensure that new or modified source code authored by Microsoft's online services staff is developed in a secure fashion, no malicious code has been introduced into the system, and that proper coding practices are followed. The reviewers' names, review dates, and review results are documented and maintained for audit purposes. A formal security quality assurance process is implemented to test for vulnerabilities to known security exposures and exploits. The process includes the use of automated security testing tools and requires that all high vulnerabilities get remediated before the system will be released to production. Patches, updates and threat mitigation are all covered by the Microsoft Security Development Lifecycle (SDL), a detailed, robust practice that Microsoft has developed over many years. Part of the SDL has been built upon investments in Microsoft Trustworthy Computing. We have various patch management release cycles and engagement models that allow us to mitigate new threats as quickly as possible within the service. Microsoft SDL Conforms to ISO/IEC 27034-1:2011
A.14.3 TEST DATA		
Objective: To ensure the protection of data used for testing.		
A.14.3.1	Test data shall be selected carefully, protected and controlled.	Microsoft requires the developer of the information system, system component, or information system

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		service to create and implement a security assessment plan. In accordance with Microsoft Security Development Lifecycle, security testing occurs in several phases throughout the SDL process. Specifically, security testing occurs during the following phases: • Phase 3 – Implementation • Phase 4 – Verification • Phase 5 – Release
A.15 SUPPLIER RELATIONSHIPS		
A.15.1 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS		
Objective: To ensure protection of the organization’s assets that is accessible by suppliers.		
A.15.1.1	Information security requirements for mitigating the risks associated with supplier’s access to the organization’s assets should be agreed with the supplier and documented.	Microsoft establishes personnel security requirements including security roles and responsibilities for third-party providers. Microsoft’s Corporate IT Policy applies across the company to all information and processes used in the conduct of Microsoft business. All employees, interns, vendors, contingent staff, partners, and business guests are accountable and responsible for complying with these guiding principles. Additionally, all Microsoft Online Services staff are required to comply with the Microsoft Security Policy and Standards. This includes those located at Microsoft subsidiaries and locations not owned by Microsoft such as offsite facilities. Contingent staff are expected to meet all Microsoft IT requirements for maintenance of passwords, confidentiality, and security procedures. Policies and Guidelines for Microsoft Temporary Workers and Vendors can be found on HRWeb. In all contracts, Microsoft includes provisions to ensure that third-party providers meet or exceed the personnel security requirements mandated by Microsoft. This includes the ability to successfully pass the Microsoft background check, or equivalent, as well as obtain and maintain a clearance if the specific project requires it. Third-party providers are subject to the same personnel screening requirements as Microsoft employees working on the Microsoft Online Services system for Federal customers. Third-party providers are required to sign a

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		Non-Disclosure Agreement prior to accessing Microsoft information systems or resident information.
A.15.1.2	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization’s information.	Microsoft requires that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Microsoft requires all third parties (external information system services) who are engaged with Microsoft Online Services to sign a Microsoft Master Vendor Agreement (MMVA). The MMVA requires the third party to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of Microsoft confidential information. Microsoft includes provisions in the MMVA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Vendors that handle sensitive data must be in compliance with Microsoft vendor privacy practices and data protection requirements.

A.15.2 SUPPLIER SERVICE DELIVERY MANAGEMENT

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

A.15.2.1	Organizations shall regularly monitor, review and audit supplier service delivery.	Microsoft employs processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. Microsoft Online Services signs Interconnection Security Agreements (ISA) with external information systems as necessary; ISAs define Microsoft Online Services oversight. Microsoft includes provisions in the Microsoft Master Vendor Agreement (MMVA) and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Vendors that handle sensitive data must be in compliance with Microsoft vendor privacy practices and data protection requirements.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.15.2.2	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Microsoft conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services. A risk assessment of third-party service providers is performed as part of all acquisitions activities. All third-party vendors are required to hold an MMVA which includes basic risk assessment of the vendor as a business. For any party with whom Microsoft signs an ISA, Microsoft meets with them regularly and monitors the agreement and any changes within the agreement. All software acquisitions (internal or external) must follow the Microsoft configuration management process.
A.16 INFORMATION SECURITY INCIDENT MANAGEMENT		
A.16.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.1	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.	Microsoft develops, documents, and disseminates to all relevant personnel or roles an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The Microsoft Security Policy defines Microsoft Online Services policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Microsoft Online Services. The Microsoft Security Policy contains rules and requirements that must be met in the delivery and operation of Microsoft Online Services. The policy is reviewed and updated at least annually. Policies and procedures are distributed to personnel with responsibilities for implementing those policies and procedures via email links to SharePoint. Microsoft Online Services has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A Security incident may include, but are not limited to: e-mail viruses, malware, worms, denial of service attacks, unauthorized access, and any other type of unauthorized, or unlawful activity

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		involving Microsoft Online Services computer networks or data processing equipment. The Microsoft Online Security Incident Response process follows the following phases: • **Identification** – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Microsoft Online operational and decurity organizations. . If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists. • **Containment** – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices. • **Eradication** – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If vulnerability is determined, the escalation team reports the issue to product engineering. • **Recovery** – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity. • **Lessons Learned** – Each security incident is analyzed to ensure the appropriate mitigations applied to protect against future reoccurrence.
A.16.1.2	Information security events shall be reported through appropriate management channels as quickly as possible.	Microsoft reports security incident information to appropriate management channels as quickly as possible. Incidents are identified through internal monitoring systems, external customer communication or internal identification. Upon identification, incidents are

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		immediately brought to the attention of the Microsoft Online Services Investigation and Response team. Tickets for the incidents are entered into the tracking system, and escalated as necessary. Contractual obligations in the Data Processing Terms of the OST require Microsoft to notify customers promptly in the event of an incident affecting their data. Security notifications are, by nature, extremely rare, sensitive, and unique. Therefore, a formal process has been developed to tailor notification to the specific incident on a case-by-case basis. Notifications could be via email, phone, broad communication, or by direct engagement, depending on the issue and impact.
A.16.1.3	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Microsoft employees and contractors are required to note and report any observed or suspected information security weaknesses in systems or services. All Microsoft Online Services' security incidents, weaknesses, and malfunctions are required to be reported by Microsoft Online Services Staff and Contractor Staff immediately. The reporting and handling of these events follow prescribed procedures pursuant to defined and implemented policy.
A.16.1.4	Information security events should be assessed and it should be decided if they are to be classified as information security incidents.	Microsoft develops an incident response plan that defines reportable incidents. Microsoft Online has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A Security incident may include, but are not limited to: e-mail viruses, malware, worms, denial of service attacks, unauthorized access, and any other type of unauthorized, or unlawful activity involving Microsoft Online computer networks or data processing equipment. The Microsoft Online Security Incident Response process follows the following phases: • **Identification** – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Microsoft Online operational and decurity organizations. . If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		Microsoft. This escalation will include product, security, and engineering specialists. - **Containment** – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices. - **Eradication** – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If vulnerability is determined, the escalation team reports the issue to product engineering. - **Recovery** – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity. - **Lessons Learned** – Each security incident is analyzed to ensure the appropriate mitigations applied to protect against future reoccurrence.
A.16.1.5	Information security incidents should be responded to in accordance with the documented procedures.	Microsoft develops, documents, and disseminates to all relevant personnel or roles procedures to facilitate the implementation of the incident response policy and associated incident response controls. Microsoft Online has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A Security incident may include, but are not limited to: e-mail viruses, malware, worms, denial of service attacks, unauthorized access, and any other type of unauthorized, or unlawful activity involving Microsoft Online computer networks or data processing equipment. The Microsoft Online Security Incident Response process follows the following phases:

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		• **Identification** – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Microsoft Online operational and decurity organizations. . If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists. • **Containment** – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices. • **Eradication** – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If vulnerability is determined, the escalation team reports the issue to product engineering. • **Recovery** – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity. • **Lessons Learned** – Each security incident is analyzed to ensure the appropriate mitigations applied to protect against future reoccurrence.
A.16.1.6	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Microsoft correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. The Microsoft Online Services service and platform teams, Cloud Security Team, and Microsoft Online Services Security Incident Response Team are responsible for managing the investigation and resolution of security incidents within Microsoft Online Services. The Microsoft Online Services Security Service Engineering team and Identity and Cloud Security Team

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		must work with other teams to ensure that security incidents are contained, eradicated, and that recovery is completed. The Product Marketing Group will work with other teams to notify customers of security incidents, where appropriate, and to initiate the Privacy Incident Response Framework process where there is a concern that a privacy breach may have occurred. While the specific activities to be performed will depend on the security incident itself, there are several critical activities that must be performed as part of the process of managing the security incident response. These activities can include preparation, detection and analysis, containment, eradication, and recovery and are detailed in the Microsoft Online Services Security Incident Response SOP. A log of the security incident response effort is a useful tool for quality assurance and continuous improvement. The Microsoft Online Services Security Incident Response Team lead investigator will include any significant details of the security incident response resulting from their investigation is reflected appropriately record tools. Additionally, the Microsoft Online Services teams listed above monitor their systems for incidents to escalate to the appropriate members of the Microsoft Online Services Security Service Engineering team if an incident is discovered.
A.16.1.7	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Microsoft implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Microsoft takes every security incident very seriously. We detect and investigate all incidents affecting us without the customer having to ask. Upon becoming aware of a security incident, we use everything that is part of our security incident response process, including forensic investigation, to track exactly what happened, which data was accessed, and by whom. The incident response team lead investigator will include any significant details resulting from the investigation to the record system.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT		
A.17.1 INFORMATION SECURITY CONTINUITY		
Objective: Information security continuity shall be embedded in the organization's business continuity management systems.		
A.17.1.1	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Microsoft develops a contingency plan for the information system that identifies essential missions and business functions and associated contingency requirements. The Microsoft Security Policy defines Microsoft Online Services policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Microsoft Online Services. The Microsoft Security Policy contains rules and requirements that must be met in the delivery and operation of Microsoft Online Services. Policies and procedures are distributed to personnel with responsibilities for implementing those policies and procedures via email links to SharePoint. As part of establishing an Information Security Management System ("ISMS") for Microsoft Online Services, a risk assessment methodology was developed to provide a structured approach to risk management and to prioritize and direct Microsoft Online Services Risk Management activities. This methodology has been designed based on the following four phases to accomplish a successful risk management process: 1. Identify – Threat, Vulnerability, and Risk identification provides the list of risks which exist in the environment and provides a basis for all other risk management activities 2. Assess – The risk assessment considers the potential impact of an information security risk to the business and its likelihood of occurrence; determine appropriate risk treatment plan to reduce risk to a desirable level 3. Report – Risk reports provide managers with the data they need to make effective business decisions and to comply with internal policies and industry regulations

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		4. Monitor – Risk groups perform testing and monitoring activities to evaluate whether processes, initiatives, functions, and/or activities are mitigating the risk as designed The Risk Assessment Assess phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level.
A.17.1.2	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Microsoft develops a contingency plan for the information system that provides recovery objectives, restoration priorities, and metrics. Plans are developed and maintained per Industry best practices to be reflective of the current production environment. For more details regarding service continuity please see the Service Description. Microsoft Online Services maintains a framework that is consistent with industry and Microsoft best practices that drives the continuity program at all levels. The Microsoft Online Services framework includes: • Assignment of key resource responsibilities • Notification, escalation and declaration processes • Recovery Time Objectives and Recovery Point Objectives • Continuity plans with documented procedures • Training program for preparing all appropriate parties to execute the Continuity Plan • A testing, maintenance, and revision process
A.17.1.3	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Microsoft regularly tests the contingency plan for the information system using exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan. Recovery plans are validated on a regular basis per industry best practices to ensure that solutions are viable at time of event. The Microsoft Online Services teams are coordinating regular failover exercises. After a failover exercise is completed for contingency planning, any findings will be documented during the post-mortem. This post-mortem contingency plan document will be updated to include the lessons learned

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		and any necessary procedural changes/enhancements to the plan.
A.17.2 REDUNDANCIES		
Objective: To ensure availability of information processing facilities.		
A.17.2.1	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Microsoft develops a contingency plan for the information system that addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure. Microsoft has redesigned the Microsoft Online Services software, service, and controls to expect, plan for, and address failures at the hardware, network, and data center levels. By building in the intelligence to handle failure at the application layer (within our own software) instead of at the data center layer (relying on third-party hardware), Microsoft Online Services is able to deliver significantly high availability and reliability. While in practice the data centers are operating somewhere between Tier 3 and Tier 4 as defined by TIA 942 (Telecommunications Industry Association) standards body, the applications are delivering against the financially-backed service level agreement (SLA) of 99.9%. The Microsoft Online Services are built with reliability as a pillar. The core reliability design principles include: 1. **Redundancy** built into every layer—physical redundancy (via multiple disk/cards, servers, geographical sites, and data centers); data redundancy (constant replication across data centers); and functional redundancy (the ability for customers to work offline when there is no network connectivity). 2. **Resiliency**, via active load balancing and dynamic prioritization of tasks based on current loads; constant recovery testing across failure domains; and both automated and manual failover to healthy resources. 3. **Distributed functionality** of component services, to help limit the scope and impact of a failure in one area

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
		and to simplify all aspects of maintenance and deployment, diagnostics, repair and recovery. 4. **Continuous monitoring**, with extensive recovery and diagnostic tools to drive automated and manual recovery of the service. 5. **Simplification** to drive predictability, including the use of standardized components and processes, wherever possible; loose coupling among the software components for less complex deployment and maintenance; and a change management process that goes through progressive stages from scope to validation before being deployed worldwide. 6. **Human backup**, with 24/7 on-call support to provide rapid response and information collection towards problem resolution.

A.18 COMPLIANCE

A.18.1 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A.18.1.1	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Microsoft develops, documents, and disseminates to all relevant personnel or roles a security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. As a service provider Microsoft Online Services focuses on how using our services can help our customers manage or meet their own compliance obligations. Microsoft is continuing to mature and enhance our risk management features to address a wider array of regulatory requirements across a broad set of industry verticals. Microsoft Online Services employs a hybrid controls framework approach to address the myriad of regulatory requirements that govern the services and data Microsoft Online Services manages for our customers. In this manner, Microsoft identifies and uses commonality to build an integrated set of specific control objectives, and drives those control objectives into a consolidated framework, enhancing efficiency and

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		improving compliance management. In this way Microsoft Online Services enhances the risk management posture of our services, as well as addresses any requirements relevant to external compliance obligations by the Microsoft Online Services services or underlying infrastructure. In some instances, non-common controls may be added conditionally where business need justifies the additional cost and complexity.
A.18.1.2	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Microsoft uses software and associated documentation in accordance with contract agreements and copyright laws. Risk associated with Intellectual Property Rights (IPR) violations are factored into the technical and procedural controls that govern Microsoft Online Services' service offerings. However, the vast majority of software used to deliver services is Microsoft product.
A.18.1.3	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.	Microsoft enforces mandatory access control policies over all subjects and objects where the policy specifies that a subject that has been granted access to information is constrained from passing the information to unauthorized subjects or objects. Microsoft Online Services owned assets are retained as appropriate based on retention requirements set by Corporate Records Management and an asset's classification, or based on contractual requirements. Microsoft guarantees retention of tenant data for 30 days after termination and all information is permanently deleted 90 days after termination of service. Please see Product Use Rights for up to date information. The classification of assets is included in the Microsoft Online Services asset inventory.
A.18.1.4	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Microsoft determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need. Microsoft Online Services owned assets are retained as appropriate based on retention requirements set by Corporate Records Management and an asset's classification, or based on contractual requirements. Microsoft guarantees retention of tenant data for 30

ISO/IEC 27001:2013 Control ID	ISO/IEC 27001:2013 Control	Microsoft Services Response
		days after termination and all information is permanently deleted 90 days after termination of service. The classification of assets is included in the Microsoft Online Services asset inventory. Microsoft Online Services has a comprehensive framework to comply with FISMA, SSAE16, HIPAA, ISO27011, EUMC, and other regulations as necessary. As part of this framework, Microsoft Online Services maintains ongoing continuous monitoring programs to assure compliance in post-production deployments.
A.18.1.5	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Microsoft implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. Microsoft Online Services leverages the cryptographic capabilities that are directly a part of the Windows operating system for certificates, and authentication mechanisms such as Kerberos. These cryptographic modules have been certified by NIST as being FIPS 140-2 complaint. Any time cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data within Microsoft Online Services, the modules and ciphers are FIPS 140-2 compliant. For additional information on how cryptographic modules are employed in Microsoft products, see TechNet article cc750357. Microsoft Online Services provides digital certificates on public facing, external websites. These certificates allow Federal users to authenticate the legitimacy of the site before establishing an encrypted connection and transferring data. For more information on Digital Certificates, refer to TechNet article cc776447 – 'How Certificates Work.'

A.18.2 INFORMATION SECURITY REVIEWS

Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

ISO/IEC 27001:2013 Control ID	**ISO/IEC 27001:2013 Control**	Microsoft Services Response
A.18.2.1	The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Microsoft develops a security assessment plan that describes the scope of the assessment including the assessment environment, assessment team, and assessment roles and responsibilities. Microsoft takes a risk-based approach to managing the cloud service. As part of our periodic independent assessments, some controls are tested continuously and others are tested multiple times a year. We provide evidence of these tests through independent ISO audits that are conducted annually.
A.18.2.2	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Microsoft regularly reviews and updates the current audit and accountability procedures. The Microsoft Security Policy contains rules and requirements that must be met in the delivery and operation of Microsoft Online Services. More detailed requirements are established within Microsoft Online Services Security Procedures and service team-specific standard operating procedures (SOPs). These standards and procedures act as adjuncts to the security policy and provide implementation level details to carry out specific operational tasks. As such, service teams regularly review their compliance with the appropriate security policies, standards, and any other security standards. Appropriate actions are taken if any non-compliance is found as a result of the review.
A.18.2.3	Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.	Microsoft regularly assesses the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements. A subset of controls will be assessed periodically to determine the extent to which the controls are implemented and operating as intended. At least one third of controls will be assessed each year, ensuring that all controls are assessed at least every three years. Other criteria, such as major system changes, and changes in risk posture and vulnerabilities, may trigger assessments.

Document type: Controlled (handed to customer under NDA when authenticated or on request)
Document stage: Published
Next review: November 2015

ISO/IEC 27018:2014 CONTROLS

ISO/IEC 27018:2014 Control ID	ISO/IEC 27018:2014 Control	Microsoft Services Response
A.1 CONSENT AND CHOICE		
A.1.1 OBLIGATION TO CO-OPERATE REGARDING PII PRINCIPALS' RIGHTS		
A.1.1	The cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct, and/or erase PII pertaining to them.	Microsoft provides a process for customers to have inaccurate personally identifiable information (PII) maintained by Microsoft corrected or amended, as appropriate. As documented in the Data Processing Terms (DPT) of the Online Services Terms (OST), the features and functionality of the Microsoft online services mean customers remain in control of customer content stored within the service.
A.2 PURPOSE LEGITIMACY AND SPECIFICATION		
A.2.1 PUBLIC CLOUD PII PROCESSOR'S PURPOSE		
A.2.1	PII to be processed under a data processing contract should not be processed for any purpose independent of the instructions of the cloud service customer.	Microsoft describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. See http://www.microsoft.com/online/legal/v2/ for the Microsoft Online Services Privacy statement.

ISO/IEC 27018:2014 Control ID	ISO/IEC 27018:2014 Control	Microsoft Services Response
A.2.2 CLOUD PII PROCESSOR'S COMMERCIAL USE		
A.2.2	PII processed under a data processing contract should not be used by the cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.	Microsoft describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. See http://www.microsoft.com/online/legal/v2/ for the Microsoft Online Services Privacy statement.
A.4 DATA MINIMIZATION		
A.4.1 SECURE ERASURE OF TEMPORARY FILES		
A.4.1	Temporary files and documents should be erased or destroyed within a specified, documented period.	Microsoft disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access. Per the Data Processing Terms of the OST, no more than 180 days after expiration or termination of Customer's use of an Online Service, Microsoft will disable the account and delete Customer Data from the account.
A.5 USE, RETENTION AND DISCLOSURE LIMITATION		
A.5.1 PII DISCLOSURE NOTIFICATION		
A.5.1	The contract between the cloud PII processor and the cloud service customer should require the cloud PII processor to notify the cloud service customer of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.	Microsoft describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. See the Data Processing Terms of the OST. Microsoft will not disclose Customer Data to a third party (including law enforcement, other government entity, or civil litigant; excluding our subcontractors) except as you direct or unless required by law. Should a third party contact Microsoft with a request for Customer Data, we will attempt to redirect the third party to request the data directly from you. As part of that process, we may provide your contact information to the third party. If compelled to disclose Customer Data to a third party, we will use commercially reasonable efforts to notify you in advance of a disclosure unless legally prohibited.

ISO/IEC 27018:2014 Control ID	ISO/IEC 27018:2014 Control	Microsoft Services Response
A.5.2 RECORDING OF PII DISCLOSURES		
A.5.2	Disclosures of PII should be recorded, including what PII has been disclosed, to whom, at what time.	Microsoft keeps an accurate accounting of disclosures of information held in each system of records under its control, including date, nature, and purpose of each disclosure of a record. If compelled to disclose Customer Data to a third party, we will use commercially reasonable efforts to notify you in advance of a disclosure unless legally prohibited.
A.7 OPENNESS, TRANSPARENCY AND NOTICE		
A.7.1 DISCLOSURE OF SUB-CONTRACTED PII PROCESSING		
A.7.1	The use of sub-contractors by the PII processor to process PII should be disclosed before their use to the relevant cloud service customers.	Microsoft evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. By default, no one has access to customer data without authorization. Our subcontractors handle this data only when required to provide or maintain the service. In the interest of transparency, we let customers know which subcontractors we use and what they do. Customers may download a current list of Office 365 subcontractors from the Microsoft Office 365 Trust Center. Customers who subscribe to compliance notifications will be notified when we add a new subcontractor to Microsoft Online Services.
A.9 ACCOUNTABILITY		
A.9.1 NOTIFICATION OF A DATA BREACH INVOLVING PII		
A.9.1	The cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII, or unauthorized access to processing equipment or facilities resulting in loss, disclosure, or alteration of PII.	The organization requires personnel to report suspected security incidents to the organizational incident response capability. Incidents are identified through internal monitoring systems, external customer communication or internal identification. Upon identification, incidents are immediately brought to the attention of the Microsoft Online Services Investigation and Response team. Tickets for the incidents are entered into the tracking system, and escalated as necessary. Contractual obligations in the Data Processing Terms of the OST require Microsoft to notify customers promptly in the event of an incident affecting their data. Security notifications are, by nature, extremely rare, sensitive, and unique. Therefore, a formal process has been developed to tailor notification to the specific incident on a case-by-case basis.

ISO/IEC 27018:2014 Control ID	ISO/IEC 27018:2014 Control	Microsoft Services Response
		Notifications could be via email, phone, broad communication, or by direct engagement, depending on the issue and impact.
A.9.2 RETENTION PERIOD FOR ADMINISTRATIVE SECURITY POLICIES AND GUIDELINES		
A.9.2	Records of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating).	Microsoft retains its security documents pursuant to its retention requirements. Microsoft Online Services owned assets are retained as appropriate based on retention requirements set by Corporate Records Management and an asset's classification, or based on contractual requirements. Microsoft guarantees retention of tenant data for 30 days after termination and all information is permanently deleted 90 days after termination of service.
A.9.3 PII RETURN, TRANSFER AND DISPOSAL		
A.9.3	The cloud PII processor should have a policy in respect of the return, transfer, and/or destruction of PII and should make this policy available to the cloud service customer.	Microsoft disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access. Per the Data Processing Terms of the OST, no more than 180 days after expiration or termination of Customer's use of an Online Service, Microsoft will disable the account and delete Customer Data from the account.
A.10 INFORMATION SECURITY		
A.10.1 CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS		
A.10.1	Individuals under the cloud PII processor's control with access to PII should be subject to a confidentiality obligation.	Microsoft ensures that individuals requiring access to organizational information and information systems containing Customer Data sign appropriate access agreements prior to being granted access. All Microsoft Online Services staff are required to sign confidentiality and non-disclosure agreements, as well as the Microsoft Employee Handbook, at the time of hire as a condition for employment. Additionally, the Microsoft Corporate General Use Standard describes user responsibilities and establishes expected behavior when using Microsoft Online Services. All users, including employees, vendors, and contractors are required to follow the rules of behavior outlined in the General Use Standard. Vendors and contractors are required to have a signed Microsoft Master Vendor Agreement (MMVA) to ensure compliance with Microsoft policies on required engagements. The agreements are

ISO/IEC 27018:2014 Control ID	ISO/IEC 27018:2014 Control	Microsoft Services Response
		put in place to protect trade secrets, sensitive, or business confidential information and assets. All Microsoft's Online Services contingent staff must also sign a non-disclosure agreement at the time of engagement and before being given access to Microsoft's Online Services.
A.10.2 RESTRICTION OF THE CREATION OF HARDCOPY MATERIAL		
A.10.2	The creation of hardcopy material displaying PII should be restricted.	Microsoft restricts access to creation of hardcopy material displaying PII. Microsoft maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. Microsoft imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities
A.10.3 CONTROL AND LOGGING OF DATA RESTORATION		
A.10.3	There should be a procedure for, and a log of, data restoration efforts.	Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and which data (if any) had to be input manually in the data recovery process. Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. Microsoft reviews data recovery procedures at least every six months.
A.10.4 PROTECTING DATA ON STORAGE MEDIA LEAVING THE PREMISES		
A.10.4	Protecting data on storage media leaving the premises	Microsoft protects and controls data on storage media during transport outside of controlled areas. For this control, digital media at Microsoft data centers consist of servers, network devices, and magnetic backup tapes. Microsoft data centers do not use non-digital media. Microsoft utilizes 3 methods to protect media that is being transported outside the data center: 1) Secure Transport 2) Encryption 3) Cleanse, Purge, or Destroy.

ISO/IEC 27018:2014 Control ID	ISO/IEC 27018:2014 Control	Microsoft Services Response
		1. All media being transported from Microsoft data centers require accurate tracking. Tickets are created to arrange and track the transportation of media. Microsoft has contracted with several approved vendors to provide secure shipping services. Secure Transport begins with an accurate inventory and chain of custody. Authorized asset managers are required to manage the exchange of assets. Assets are inventoried at the time of delivery to the transporter. The asset manager must witness the container being locked and a tamper proof seal applied. Secure Transport could have additional requirements such as a dedicated transport for only Microsoft assets, GPS tracking, and only stopping at Microsoft locations. In cases of longer transport routes, the requirement could be that there are multiple drivers and trucks with sleeping quarters to provide for non-stop delivery. At the delivery location, the transport company's approved personnel must be present to witness the removal of the tamper proof seal and unlocking of the container. The receiving personnel will inventory the shipment and send a message confirming the receipt of the assets. This inventory is validated by the Microsoft asset manager. 2. Some assets are required by Microsoft to be encrypted during transport. Magnetic backup tapes are required to be encrypted. DPS utilizes SafeNet KeySecure to manage cryptographic keys using a FIPS 140-2 Level 3 validated encryption module (cert# 1694) and HSM (cert#1178) to secure AES 256-bit encrypted data on the magnetic tapes. When magnetic tapes are picked up for offsite storage, an approved asset manager must deliver the locked container to the offsite storage vendor and enter an account pin before inventorying the tapes being transported. Upon receipt of by the storage vendor, a message confirming the inventory received is sent to the asset manager. 3. Microsoft contracts with a vendor to provide equipment destruction. Depending on Microsoft asset classification some equipment is required to be destroyed onsite. All Microsoft assets are required to be cleansed or purged before leaving the data center Microsoft assets are cleansed/purged with methods consistent with NIST SP 800-88 prior to reuse or disposal. Microsoft utilizes data erasure units from Extreme Protocol Solutions (EPS). EPS software supports NIST SP 800-88 requirements for cleansing and purging/secure erasure. Prior to cleansing or destruction, an inventory is created by the Microsoft asset manager. If a vendor is used for destruction, the vendor

ISO/IEC 27018:2014 Control ID	ISO/IEC 27018:2014 Control	Microsoft Services Response
		provides a certificate of destruction for each asset destroyed, which is validated by the asset manager.
A.10.2 RESTRICTION OF THE CREATION OF HARDCOPY MATERIAL		
A.10.5	Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.	Microsoft disallows removable media and wireless devices in our data centers, but for emergency reasons (such as in case of fire) and to enable people to do their jobs, mobile phones are allowed. However, if such a device were to be attached to physical hardware, this action would trigger a security alert. Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities.
A.10.6 ENCRYPTION OF PII TRANSMITTED OVER PUBLIC DATA-TRANSMISSION NETWORKS		
A.10.6	PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.	Microsoft implements cryptographic mechanisms to prevent unauthorized disclosure of information during transmission. Microsoft encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. Microsoft utilizes FIPS 140-2 SSL/TLS encryption for all connections that travel outside the boundary of Microsoft Online Services. SSL/TLS employs cryptographic mechanisms that allow client/server applications to communicate across the network in a way designed to prevent eavesdropping and tampering. Microsoft Online Services MultiTenant's FIPS 140-2 encryption modules used for transmitted information are certified by NIST via certificates 1334, 1335, and 1336. Connections within the accreditation boundary occur within Microsoft facilities. Since Microsoft owns and controls access to these connections, they do not require FIPS 140-2 encryption
A.10.7 SECURE DISPOSAL OF HARDCOPY MATERIALS		
A.10.7	Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	In the Microsoft Online Service data center environment, digital media is required to be cleansed/purged using approved tools and in a manner consistent with NIST SP 800-88 prior to being reused or disposed of. Non-digital media is not used by the data center environment.
A.10.8 UNIQUE USE OF USER IDS		
A.10.8	If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.	Microsoft uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Microsoft Online Services properties uniquely identify and authenticate Microsoft organizational users through the use of multiple Active Directory deployments.

ISO/IEC 27018:2014 Control ID	ISO/IEC 27018:2014 Control	Microsoft Services Response
		Operations staff needing to perform administrative functions must access the environment remotely by design. Operations staff are identified by the Active Directory username specific to each property's environment, and authenticate using a strong password or two factor authentication.
A.10.9 RECORDS OF AUTHORIZED USERS		
A.10.9	An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.	Microsoft specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account. Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data. The Microsoft Security Policy prohibits the use of guest/anonymous and temporary accounts. All account requests go through the standard account management process. Account changes are managed with automated workflow management tools that allow service teams to track the process through account request, approval, creation, modification, and deletion. From a people and process standpoint, Microsoft's presume breach practices involves 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) of engineer privileges to troubleshoot the service. An access approver role reviews and approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed.
A.10.10 USER ID MANAGEMENT		
A.10.10	De-activated or expired user IDs should not be granted to other individuals.	Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. All account requests go through the standard account management process. Account changes are managed with automated workflow management tools that allow service teams to track the process through account request, approval, creation, modification, and deletion. Terminated users are removed from Corp AD; as the regular AD sync occurs, this also removes them from service team AD. Additionally, service team management is notified of terminations and transfers and removes users as needed.

ISO/IEC 27018:2014 Control ID	ISO/IEC 27018:2014 Control	Microsoft Services Response
A.10.11 CONTRACT MEASURES		
A.10.11	Data processing contracts between the cloud service customer and the cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data is not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the cloud PII processor.	Microsoft, where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used. In the interest of transparency, we let customers know which subcontractors we use and what they do. Customers may download a current list of Office 365 subcontractors from the Microsoft Office 365 Trust Center. Customers who subscribe to compliance notifications will be notified when we add a new subcontractor to Microsoft Online Services. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the Data Processing Terms of the OST.
A.10.12 SUB-CONTRACTED PII PROCESSING		
A.10.12	Data processing contracts between the cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.	Microsoft requires that providers of external information system services comply with Microsoft information security requirements in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Microsoft requires all third parties (external information system services) who are engaged with Microsoft Online Services to sign a Microsoft Master Vendor Agreement (MMVA). The MMVA requires the third party to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of Microsoft confidential information. Microsoft includes provisions in the MMVA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Vendors that handle sensitive data must be in compliance with Microsoft vendor privacy practices and data protection requirements. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the Data Processing Terms of the OST.
A.10.13 ACCESS TO DATA ON PRE-USED DATA STORAGE SPACE		
A.10.13	The cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that	Microsoft prevents unauthorized and unintended information transfer via shared system resources. Per the Data Retention policies in the Data Processing Terms of the OST, Microsoft uses industry standard processes to delete Customer Data when it is no longer needed. Microsoft uses best

ISO/IEC 27018:2014 Control ID	ISO/IEC 27018:2014 Control	Microsoft Services Response
	storage space is not visible to the cloud service customer.	practice procedures and a wiping solution that complies with [NIST 800-88]() (National Institute of Standards & Technology Special Publication 800-88, Guidelines for Media Sanitization).

A.11 PRIVACY COMPLIANCE

A.11.1 GEOGRAPHICAL LOCATION OF PII

A.11.1	The public cloud PII processor should specify and document the countries in which PII might possibly be stored.	Microsoft establishes, maintains, and updates an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII). See the Location of Customer Data at Rest policies in the [Data Processing Terms of the OST.]()

A.11.2 INTENDED DESTINATION OF PII

A.11.2	PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.	Microsoft protects the confidentiality and integrity of transmitted information. All encryption modules are operated in FIPS mode which has been FIPS 140-2 certified. This ensures the confidentiality and integrity of communications between services teams, partners, and customers are protected. Microsoft provides FIPS 140-2 cipher support for customer, third party, and remote access connections into the FISMA accreditation boundary. Microsoft services utilize FIPS 140-2 SSL/TLS encryption for all connections that travel outside the boundary of Microsoft Online Services. SSL/TLS employs cryptographic mechanisms that allow client/server applications to communicate across the network in a way designed to prevent eavesdropping and tampering.