

Microsoft Azure

Responses to Motion Picture Association of America Common Guidelines

**http://www.microsoft.com/trust**

NOTE: Certain recommendations contained herein may result in increased data, network, or compute resource usage, and increase your license or subscription costs.

*Version 1, Published March 2016*

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

(c) 2016 Microsoft Corporation. All rights reserved. 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. Some examples are for illustration only and are fictitious. No real association is intended or inferred.

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

Table of Contents

[1 Introduction 4](#_Toc446067734)

[1.1 About This Document 4](#_Toc446067735)

[Microsoft Azure Responses to MPAA 2015 Common Guidelines 6](#_Toc446067736)

[Management System 6](#_Toc446067737)

[Physical Security 11](#_Toc446067738)

[Digital Security 22](#_Toc446067739)

[2 References and Further Reading 41](#_Toc446067740)

# Introduction

Content security and protection is critical for feature film development, as there are multiple points in the workflow where digital assets can be compromised or stolen. Dailies, rough cuts, and visual effects are just some of the materials exposed during normal production, and the box-office impacts of a security breach on a blockbuster project can reach tens of millions of dollars.

At the same time, production IT systems (in-house / on-premises or rented) remain a significant overhead expense for studios—one they would like to minimize while still protecting highly valuable content. By moving workflows into the Microsoft Azure public cloud, producers and content creators can enhance the security of their productions and:

* Offload the burdens of content protection and compliance to Azure;
* Take advantage of Microsoft’s decades of experience in security development, enterprise datacenters, and services;
* Use the scale and presence of Azure to enable global collaboration with ease;
* Burst high-demand traffic to the cloud for rendering, encoding, encryption, and more.

To help major studios, partners, and vendors design infrastructure and solutions that ensure the security of digital film assets, the [Motion Picture Association of America](http://www.mpaa.org/) (MPAA) provides best-practices guidance and security control frameworks. The MPAA also performs content security assessments on behalf of its member companies (Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, and Warner Bros. Entertainment Inc.).

Microsoft Azure is the first hyper-scale, multi-tenant public cloud to successfully complete a security and compliance assessment by the MPAA’s independent auditors. This means that companies who do business with major studio film productions can use Azure to help reduce the IT costs normally associated with secure content creation, management, and distribution.

Azure complies with the MPAA’s best-practices guidelines for application and cloud security, covering the following services: Azure AD, ACS, Batch, Cache, CDN, ExpressRoute, Event Hubs (Service Bus), Import/Export Services, Media Services, Portal, Premium Storage, Scheduler, SQL DB, Storage, Storage Files, Virtual Machines, Virtual Networks, and WorkFlow.

## About This Document

While the [audit reports](mailto:contentsecurity@mpaa.org) are only distributed by the MPAA, the [guidelines are publicly available](http://www.mpaa.org/content-security-program/) (to go through an assessment, the service provider answers the questionnaires that detail the features, processes, and policies that ensure customer data security).

This “Common Guidelines” document, and its companion “Azure Responses to MPAA Application and Cloud Security Guidelines”, provide the framework for evaluating Azure’s capabilities to support secure content workflows in the cloud. The details presented below enable deep insight into core Azure operations and architecture, such as physical security, infrastructure management, privacy policies, business continuity, and more.

You will note that some responses are shaded blue. This indicates a question or control objective that is either the customer’s responsibility, or one that is distributed between the customer and Azure. For example, user data classification is up to the customer and how it defines security boundaries on content, but Azure also has system data that is classified according to Microsoft’s information security management policy. Azure provides features that customers can use to classify data, but does not itself classify a customer’s data within an Azure Storage account.

For more information about the MPAA frameworks and best-practices guidelines, please visit <http://www.mpaa.org/content-security-program/>.

Microsoft Azure Responses to MPAA 2015 Common Guidelines

# Management System

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Control IDs** | **MPAA Guidelines** | **Microsoft Azure Response** | | | |
| **Yes** | **No** | **N/A** | **Notes** |
| **Q. 100:**  MS-1.0  MS-3.0 | *Do you have an information and content security policy/framework?* | X |  |  | Azure has established an Information Security Forum comprising a cross-functional committee of management which provides broad perspective and direction for security strategy, information security, and compliance related matters. In addition, the Information Security Forum representatives provide governance and oversight of the information security management program (ISMP). |
| **Q. 100A:**  MS-1.0  MS-3.0 | *Do you have information and content security job positions with well-defined responsibilities?* | X |  |  | Management has established defined roles and responsibilities to oversee implementation of the information security policy across Azure. |
| **Q. 101:**  MS-4.0 | *Do you have policies and procedures for content security and asset protection?* | X |  |  | Microsoft Azure has designed and implemented an information security management system (ISMS) framework that addresses industry best-practices for information security and privacy. The ISMS has been documented and communicated in a customer-facing Information Security Policy, which is available through the Service Trust Portal (<https://www.microsoft.com/en-us/TrustCenter/STP/default.aspx>). |
| **Q. 102:**  MS-6.0 to MS.6.1 | *Do you have a business continuity and disaster recovery plan, which includes a defined business continuity team?* | X |  |  | Business Continuity Plans (BCPs) have been documented and published for critical Azure services, which provide roles and responsibilities with detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RPO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.  The BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly. |
| **Q. 103:**  MS-7.0 | *Do you have change control policies and procedures?* | X |  |  | Operational Security Assurance (OSA) is a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft, including the Microsoft Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape. OSA combines this knowledge with the experience of running hundreds of thousands of servers in data centers around the world. Microsoft uses OSA to minimize risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are actually being followed effectively. When issues arise, a feedback loop helps ensure that future revisions of OSA contain mitigations to address them.  The foundation of secure online services consists of the following elements:   * SDL, to ensure the software that underlies the service is designed and developed with security in mind throughout its entire lifecycle. * OSA, to ensure the deployment and operation of the service includes effective security practices throughout its lifecycle.   The OSA process also uses feedback from online service teams within Microsoft to continuously evaluate and improve the OSA process. This feedback is also considered confidential, and it is protected in accordance with Microsoft internal policies.  The three key processes of OSA are:   * Ensuring that OSA inputs (such as organizational learning, threat intelligence, and security technologies) are up-to-date and relevant. * Developing and applying centralized review processes to consolidate all requirements to establish the OSA baseline requirements. * Engaging and implementing the new requirements and baselines.   Customers also have access to third party audit reports and certifications that encompass the controls relevant to security in development and support processes which encompass quality assurance. |
| **Q. 104:**  MS-5.0 to 5.3  DS-9.3 | *Do you have an incident response plan that establishes an incident response team, reporting procedures, response processes, and security breach notifications?* | X |  |  | Microsoft Azure has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A security event may include, among other things, unauthorized access resulting in loss, disclosure or alteration of data.   The Microsoft Azure Incident Response process follows the following phases:   * **Identification** – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Microsoft operational and security 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. |
| **Q. 105:**  MS-1.1  MS-1.3  MS-4.1 | *Do you review information and content security policies on an annual basis?* | X |  |  | Azure performs and annual review and audit of its ISMS and results are provided to management. Metrics regarding information security events are reviewed by management teams on an ongoing basis and at least monthly.  This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. |
| **Q. 106:**  MS-10.0 | *What types of background checks (employment, criminal history, credit, drug screening, etc.) do you conduct for persons (new employees, contractors, interns, third-parties, etc.) that work at your facility? (Please provide details in the comments box)* |  |  |  | All Microsoft employees and vendors who have information system access undergo screening prior to being authorized. Microsoft requires full time employees (FTEs) and vendors to undergo a background check as part of the Microsoft HR hiring practices. Background checks are required for new hires or personnel transferring to positions that involve access to customers’ work sites and/or sensitive areas, including access to customer PII. Background checks are also required due to contractual requirements with certain customers and are reviewed on a regular basis. |
| **Q. 107:**  MS-11.0 to MS-12.2 | *Do all employees, contractors, and third-party workers sign a confidentiality agreement upon hire and annually thereafter?* | X |  |  | The Microsoft Master Vendor Agreement (MMVA) requires that the third party comply with all applicable Microsoft security policies and, implement security procedures to prevent disclosure of Microsoft confidential information, and implement their own information security program. In addition to the standard security clauses included in the MMVA, third parties are expected to adhere to the following security requirements:   * All third party service providers must comply with Microsoft security and privacy policies and standards; * All third party service providers should follow the requirements stated in the Microsoft Vendor Code of Conduct document; and * All third party service providers (including Off-Facility (OF) third party personnel) are be required to take security and privacy training annually. |
| **Q. 107A:**  MS-11.0 to MS-12.2 | *Does the agreement include requirements for handling and protecting content, and returning content upon termination of the relationship?* | X |  |  | Based on the services to be provided, the Microsoft Azure manager is responsible for ensuring that the contract with the third party service provider has signed the appropriate Information Exchange Agreements (IEAs), which include confidentiality, privacy, and security requirements. The IEAs include a Non-Disclosure Agreement (NDA), Input Agreement (IA), and Technical Documentation Agreement (TDA). |
| **Q. 108:**  MS-4.2 | *Do employees, contractors, and vendors have to sign-off that they have read content security and asset protection policies and procedures?* | X |  |  | All personnel must complete annual security training to learn about Azure security and compliance requirements including security policies and standards. Training also supports important security initiatives and the awareness and mitigation of top risks.   All Azure employees must complete the mandatory training along with role-based training. |
| **Q. 109:**  MS-1.2  MS-4.3 | *Do management, employees, and contractors receive training on security (content security, security awareness, cybersecurity, Internet usage, etc.) on an annual basis?* | X |  |  | All appropriate Microsoft staff take part in Azure and/or Microsoft Cloud Infrastructure Operations (MCIO)-sponsored security training programs, 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. An example of an internal training is Microsoft Security 101. Microsoft also has non-disclosure provisions in our employee contracts.  All Azure and/or MCIO staff are required to take training determined to be appropriate to the services being provided and the role they perform. |
| **Q. 109A:**  MS-4.0  MS-1.2 | *Do you have social media policies or guidelines that address the following: how employees are allowed to associate themselves with the facility; prohibit the sharing of sensitive information or content to the outside online community; and standards of behavior?* | X |  |  | All appropriate Microsoft staff take part in Azure and/or MCIO-sponsored security training programs, 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. An example of an internal training is Microsoft Security 101. Microsoft also has non-disclosure provisions in our employee contracts.  All Azure and/or MCIO staff are required to take training determined to be appropriate to the services being provided and the role they perform. |
| **Q. 110:**  MS-8.0 to 8.1 | *Do you have documented workflows tracking content and authorization checkpoints for the following: delivery, ingest, movement, storage, removal and destruction?* | X |  |  | The customer is responsible for secure workflow processes surrounding data uploaded and processed within their Azure subscription environment. Customers can take advantage of native dynamic encryption within Azure Media Services (up to AES 256) or pre-encrypt data prior to upload into Azure storage.  However, for content assets handled by Microsoft through services such as Azure Import / Export, processes are in place for the secure receipt, processing, and return of physical hard drives submitted to an Azure datacenter. This includes segregated, caged storage with restricted access, secure server media connections, and monitored facilities at all points. |
| **Q. 110A:**  MS-8.0 to 8.1 | *Do you review and update documented workflows for changes in process on an annual basis?* | X |  |  | Information security management plans are reviewed annually and updated as needed. |
| **Q. 111:**  MS-2.0 to MS-2.1 | *Do you perform a risk assessment for content workflows and sensitive assets on an annual basis?* | X |  |  | Azure has adopted information classification schemes consistent with the Microsoft Operating Systems division. Information is classified into three categories in consideration of criticality and sensitivity, including supplemental categories for customer content (e.g., customer secrets, email bodies, storage data) or personally identifiable information (e.g., customer contact information, usernames, IP address).  Microsoft Azure performs an annual risk assessment. As part of the overall ISMS framework, baseline security requirements are constantly being reviewed, improved and implemented. Microsoft Azure's controls for risk and vulnerability assessment of the Azure infrastructure meet the requirements of the standards against which the audit reports we have identified on the Azure website at: <https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx> |

# Physical Security

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Control IDs** | **MPAA Guidelines** | **Microsoft Azure Response** | | | |
| **Yes** | **No** | **N/A** | **Notes** |
| **Q. 200:**  PS-2.0 to PS-2.3  PS-3.0 | *Do you require employees, contractors, freelance, part-time employees, and other personnel to be issued a photo identification badge when they start employment?* | X |  |  | Applies to: Employees, Contractors  Microsoft issues Smartcard photo identification to all FTEs and contractors provisioned with physical building access. |
| **Q. 201:**  MS-12.5 | *Do you require third parties (outsourced IT, cleaning crews, maintenance personnel, visitors, etc.) to sign a visitor log, be issued a visitor badge, and be restricted from areas with production content (e.g. vault, mastering rooms, screening rooms)* | X |  |  | Applies to: Cleaning Crews, Maintenance Personnel, Visitors, Others  All persons who enter the Data Center must have access requested through the Data Center Access Tool (DCAT). DCAT is the main source of record for visitors and the logging of their access.  Third-Parties are given least-privilege rights into areas that are required for them to complete their work. If their access is submitted into DCAT as a visitor, they must be escorted throughout the building at all times. |
| **Q. 202:**  MS-12.5 | *What areas in the facility do you require third parties be escorted by an authorized employee?* | X |  |  | If a third-party individual is on a visitor request, they will be issued a paper badge and must be escorted throughout the facility. If a third-party individual is given temporary access, their ID badge will only give them access into rooms for which they have approved access. |
| **Q. 203:**  MS-12.6 | *Do you notify the client studio and obtain approval, before content is offloaded to a subcontractor or another company?* |  |  | X | Data stored in Azure is owned, controlled, and accessed by the customer. Customers select and control data regions, data redundancy / replication, and offload--Microsoft does not use third-party content storage.  Azure employees only access customer data upon management approval through logged and audited processes for designated customer support purposes. |
| **Q. 204:**  PS-1.0  PS-1.2 | *Do you secure all entry/exit points to the facility, including windows, doors, and loading docks with access controlled doors?* | X |  |  | Electronic access control devices are installed on doors separating the reception area from the facilities’ interior to restrict access to approved personnel only. Datacenter lobbies have man-trap portal devices that require access card and biometric hand geometry to pass beyond the lobby.  Pre-approved deliveries are received in a secure loading bay and are monitored by authorized personnel. Loading bays are physically isolated from information processing facilities.  CCTV is used to monitor physical access to data centers and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities.   Microsoft data centers all receive SSAE16/ISAE 3402 Attestation and are ISO 27001 Certified. |
| **Q. 205:**  PS-4.0 to PS-4.3 | *Does your facility utilize physical perimeter protection?*  *If yes, please provide details such as fencing, walls, gates, security patrols, etc.* | X |  |  | Applies to: Fencing, Walls, Lighting, Window Grates, Security Patrols, Other (including Cameras, SOC, motion detectors, electrified fencing, door sensors). |
| **Q. 206A:**  PS-1.1 | *Do you require rooms used for screening purposes to be access-controlled?* |  |  | X | Azure does not access customer data. |
| **Q. 206B:**  PS-1.1 | *Do you control access to areas where content is handled by segregating the content area from other facility areas (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication and mastering)?* | X |  |  | Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. Security verification and check-in are required for personnel requiring temporary access to the interior data center facility including tour groups or visitors.  Access authorizations for data centers are managed using an authorized access list of personnel, which has been approved by the Datacenter Management team. Physical keys and access badges are stored within the Security Operations Center and inventoried multiple times per day. |
| **Q. 207:**  PS-5.0 to PS 5.2 | *Does your facility have intruder alarms?  If yes, please describe the types of intruder alarms being utilized (e.g., door sensors, motion detectors, glass break sensors, etc.) and note areas covered (entries, exits, storage, vaults, windows, etc.).* | X |  |  | All facility entry and exit points are monitored throughout the day and alarms are present and activated during non-business hours. Emergency exits are alarmed and under video surveillance. |
| **Q. 208:**  PS-5.3 | *Have you configured your alarm systems to notify security directly and/or the police and other relevant personnel (i.e. incident response team)?* | X |  |  | Escalation procedures, including requirements for contacting law enforcement, are clearly defined and provided to all security personnel as part of the Microsoft Incident Response Plan. |
| **Q. 209:**  PS-5.4 to PS.5.5 | *Do you restrict the alarm system to authorized personnel with unique arm and disarm codes for each individual?* | X |  |  | Alarms and alarm codes are managed through a combination of controls including separation of duties, automation, redundant verification, and the principle of least privilege.  Physical security responsibilities are clearly assigned to specific job roles, including alarm arming and disarming. |
| **Q. 210:**  PS-5.4 to PS.5.5 | *Do you review or update this access quarterly or when there is a change in personnel?* | X |  |  | All access to the datacenter is immediately revoked when a user has transferred or is no longer with Microsoft.  Microsoft also performs a Quarterly Access Review (QAR) using DCAT as the source of record. Users must be reviewed by data center management and all changes must be reviewed and approved before closing the QAR. |
| **Q. 211:**  PS-5.6 | *Do you test the alarm system on a quarterly basis?* | X |  |  | The data center alarm system is 24/7/365. Alarms are monitored in real-time by our Lenel system, along with our DCAT tool. Any maintenance done on the alarm system is performed under dual-control, and alarms are tested once they are brought back online. All testing and maintenance is documented and retained in accordance with Microsoft legal information retention policies. |
| **Q. 212:**  PS-5.7 | *During a power outage, do fire doors fail shut in restricted areas and fail open in other areas?* | X |  |  | Datacenters have mitigated the risk of power outages by having dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators. Data centers have made arrangements for emergency fuel delivery.  Datacenters have dedicated Facility Operations Centers to monitor the following: Power systems, including all critical electrical components, generators, transfer switches, main switch gear, power management module and uninterruptible power supply equipment. |
| **Q. 212A:**  PS-6.0 to PS-6.2 | *Do you have a process to manage facility access?* | X |  |  | Procedures have been established to restrict physical access to the datacenters to authorized employees, vendors, contractors, and visitors. Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility, including tour groups or visitors.  Access authorizations for datacenters are managed using an authorized access list of personnel, which has been approved by the Data Center Management team. Physical keys and access badges are stored in secure locations within the datacenter and inventoried multiple times per day. |
| **Q. 212B:**  PS-6.0 to PS-6.2 | *Is access for restricted areas restricted to authorized personnel?* | X |  |  | Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.  Access authorizations for data centers are managed using an authorized access list of personnel, which has been approved by the Data Center Management team. Physical keys and access badges are stored within the Security Operations Center and inventoried multiple times per day. |
| **Q. 213:**  PS-7.0 to PS-8.5 | *How do you control access into the facility (keys, electronic card, pin locks, biometrics, etc.)?* | X |  |  | Applies to: Keys, electronic cards / fobs, pin locks, biometrics. Other  Access to the data center facilities is restricted. The main interior and reception areas have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. Rooms within the Microsoft datacenter that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are restricted through various security mechanisms such as electronic card access control, keyed lock, anti-tailgating and/or biometric devices. |
| **Q. 214:**  PS-7.0 to PS-8.5 | *Do you have a process for tracking issued keys, retrieving keys back from terminated employees or persons who no longer need access, and re-keying locks / disabling access for lost keys?* | X |  |  | All Physical Keys are tracked using a combination of DCAT, physical security control systems, and the SOC key box. Approval to check-out keys is submitted, reviewed, and approved through the DCAT system. Key inventory is reviewed every shift change.   Processes are in place to retrieve keys that have not been checked back in. If not successful, a procedure is in place to re-key a rack or in the event of a facility key, rekeying the entire facility.  Microsoft Corporate Human Resources Policy drives employee termination processes and Microsoft Policy clearly defined roles and responsibilities. Termination policies and procedures cover all aspects of separation including return of assets, badges, computer equipment and data. Human Resources also manages revocation of access to all resources, both physical and electronic. |
| **Q. 215:**  PS-10.0 to PS-10.3 | *Do you log and review daily electronic access for the following restricted areas: masters/stampers vault, pre-mastering, server/machine room, scrap room, high-security cages; and weekly for all other areas?* | X |  |  | Access to all facility rooms is logged in real-time. If access to those areas is not granted, an alarm will sound in the Security Operations Center, and an immediate security dispatch will occur. |
| **Q. 216:**  PS-9.0 to PS-9.1 | *Does your facility utilize security cameras (CCTV)? If yes, how many cameras are installed throughout the facility?* | X |  |  | The total number of cameras varies from datacenter to datacenter, but all entry/egress points, as well as the surrounding perimeter, loading bays, and select areas within the facility (such as at fire doors and storage areas) are covered. |
| **Q. 216A:**  PS-9.0 to PS-9.1 | *Do the cameras cover restricted areas and entry/exit points (e.g. server room, vault, areas where content is stored or handled)?* | X |  |  | CCTV is used to monitor physical access to datacenters and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities. |
| **Q. 216B:**  PS-9.0 to PS-9.1 | *Are the areas of camera coverage well lighted, utilize motion activated lights, or infrared or low-light capable?* | X |  |  | All areas of camera coverage have proper lighting, along with emergency lighting in the case of a power outage. These lights are run off of a separate emergency panel, so that lighting is on during the change over from UPS to on-premises generators.  In some facilities, lighting is dimmed if no movement has been detected in a certain time period. Those lights have been reviewed and verified that the level of lighting is still sufficient for CCTV coverage. |
| **Q. 217:**  PS-9.1 | *What is the image resolution and frame rate of the CCTV system? (Please specify in the comments box to the right)* | X |  |  | Image specifications vary across facilities depending on location security requirements and vendor installations (for leased datacenters). |
| **Q. 218:**  PS-9.2 | *Do you place the DVR for the CCTV system in a secure access-controlled location (e.g., computer room, locked closet, and cage)?* | X |  |  | All access and attempted access to electronic badge-protected doors is centrally logged and audited on an exception basis. Automated tools alert the appropriate personnel if a security event is detected. |
| **Q. 219:**  PS-9.3 | *Do you retain CCTV data for a period of at least 90 days?* | X |  |  | All CCTV footage is retained for a minimum of 90 days. |
| **Q. 219A:**  PS-9.3 | *How often is CCTV data retention and CCTV image capture quality verified? (Please specify in the comments box to the right)* | X |  |  | All CCTV data is verified during investigations, along with upgrades of the system. |
| **Q. 220:**  PS-11.0 to PS-11.4  PS-11.7  PS-11.8 | *Do you have policy and procedures for searching all personnel and visitors that exit the building and also when entering and exiting restricted areas, for client content?* |  | X |  | All individuals who enter the facility must agree to the Microsoft Datacenter work site rules. These rules dictate what can be brought into and out of the building. |
| **Q. 221:**  PS-11.6 | *Do you periodically audit and find ways to improve the search process?* |  | X |  | Microsoft does not employ a search process within our fully managed sites. |
| **Q. 222:**  PS-11.9 | *If your facility performs Replication, do you review the exit search process for security guards upon exit?* |  |  | X | Azure does not provide media replication services. |
| **Q. 222A:**  PS-11.9 | *If your facility performs Replication, do you segregate security guard responsibilities (search process) for overseeing plant/production areas from exit points?* |  |  | X | Azure does not provide media replication services. |
| **Q. 224:**  PS-12.1 | *Do you have a content asset management system that tracks content assets using barcodes or unique tracking identifiers? If yes, please describe the details of the information that the asset management system records. (Please specify in the comments box to the right)* | X |  |  | Asset Management is owned by the Datacenter Logistics teams. They use a combination of internal tools to track all assets from acquisition, installation, deployment, management, and retirement of infrastructure assets. Asset IDs are affixed to all assets and are scanned into the system and throughout the lifecycle of an asset. |
| **Q. 225:**  PS-12.2, PS-12.4, PS-12.5 | *Does the content asset management system perform the following: track asset movements, use alias in place of studio names, create a daily aging report for assets checked out and not returned?* |  |  | X | Azure does not provide asset management, processing, or tracking for customer content, and as such does not use a check-in/check-out mechanism.  Customers may use the Azure Import/Export Service for bulk-upload and download of digital content into/from their subscription, and all handling of physical media (hard drives) is monitored and logged. Media is stored securely in locked cages and may not be accessed by anyone but authorized Azure support personnel. Customer media is only keep on-site during the transfer process, and is immediately returned to the customer upon completion. |
| **Q. 226:**  PS-12.3 | *Do you review content asset management logs at least weekly?* |  |  | X | Customers are responsible for managing content and digital assets within their subscription environment. Azure provides mechanisms for logging access to files, applications and data (such as Azure Diagnostics Services).  Azure infrastructure information is managed according to the ISMS, and follows industry best-practices for document security. |
| **Q. 226A:**  PS-12.3 | *Does the review include an investigation of anomalies?* |  |  | X | Please see response to Question 226 above. |
| **Q. 227:**  PS-13.0-PS-13.1 | *How frequently are inventory counts performed and reconciled with records in the content asset management system?* | X |  |  | Asset Inventory counts are performed quarterly by the logistics team on site. Assets on-site (scanned and records) are compared to physical observations (Tile, Row, Colo, etc.). These results are reviewed by data center management and any issues are resolved and a new test is performed. |
| **Q. 228:**  PS-12.6 | *Do you lock up assets if shipments are delayed or returned?* |  |  | X | Azure does not handle customers' physical assets.  Infrastructure devices such as servers, hard disks, or network systems are kept in secure loading bays prior to deployment, as well as upon decommissioning / destruction. |
| **Q. 229:**  PS-14.0, PS-14.2 | *Do you store blank media and raw stock in a secured location (e.g., locked cabinet, safe etc.)?* |  |  | X | Azure does not produce physical media, and does not keep such resources on-site.  However, customers using the Azure Import/Export service have their physical drives kept in locked and monitored cages until they are processed and returned. |
| **Q. 230:**  PS-14.1 | *Do you track (reconcile existing raw stock with work orders) the consumption of raw materials on a monthly basis?* |  |  | X | Azure does not produce physical media. |
| **Q. 232:**  PS-15.1 | *Do you store client assets in a secure physical location (e.g., locked cabinet, safe etc.)?* |  |  | X | Azure does not produce physical media, and does not keep such resources on-site.  However, customers using the Azure Import/Export service have their physical drives kept in locked and monitored cages until they are processed and returned. |
| **Q. 233:**  PS-15.1 | *Do you have the capability to segregate high security assets from other assets in storage upon client request?* | X |  |  | Customers are responsible for ensuring appropriate access controls and encryption are used for the assets they store in their Azure subscription. Azure provides the mechanisms for securing digital content, and ensures data isolation through mechanisms such as Storage Access Keys, BitLocker volume encryption, Azure Rights Management, PlayReady, and others. |
| **Q. 237:**  PS-16.1 | *Do you have a documented asset disposal policy?* | X |  |  | Customers are responsible for enforcing their own data retention policies. Microsoft Azure provides tools to securely delete data including immediately removing the index from the primary location, and removal of any geo-replicated copies of the data (index) asynchronously. Media wiping is NIST 800-88 compliant, defective disks are destroyed, and customers can only read from disk space to which they have previously written.  [see http://blogs.msdn.com/b/walterm/archive/2012/02/01/windows-azure-data-cleansing-and-leakage.aspx] |
| **Q. 238:**  PS-16.0 to PS-16.1 | *Do you store rejected, damaged, and obsolete stock containing client assets in a secure location before they are erased, degaussed, shredded, or physically destroyed before disposal?* |  |  | X | Microsoft does not provide media production services.  Microsoft uses best practice procedures and a media wiping solution that is NIST 800-88 compliant. For hard drives that can’t be wiped we use a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. Microsoft Azure services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle. |
| **Q. 239:**  PS-16.1 | *"Do you dispose of rejected, damaged, and obsolete stock?*  *If yes, what methods are used for disposal (e.g. degaussing, shredding or physically destruction)?"* |  |  |  | Applies to: Degaussing, Shredding, Physical Destruction, other  Data destruction techniques vary depending on the type of data object being destroyed, whether it is subscriptions, storage, virtual machines, or databases. In Azure's multi-tenant environment, careful attention is taken to ensure that one customer’s data is not allowed to either “leak” into another customer’s data, or when a customer deletes data, no other customer (including, in most cases, the customer who once owned the data) can gain access to that deleted data.  Azure follows NIST 800-88 Guidelines on Media Sanitization, which address the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization. |
| **Q. 240:**  PS-16.2 | *Do you maintain a log of items slated for disposal or destruction?* | X |  |  | For hard drives that can’t be wiped we use a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. Microsoft Azure services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle. |
| **Q. 240A:**  PS-16.2 | *If you answered “yes” to question 240, is the log kept for at least twelve months?* | X |  |  | Logs of all destruction are stored for at least 12 months, in compliance with Microsoft’s legal information retention policies |
| **Q. 241:**  PS-16.3 | *Do you destroy assets on-site with supervision and signed-off by two company personnel?* | X |  |  | All assets are destroyed on-site with dual control. Assets are first verified by a Microsoft full-time employee, and then verified by the third-party destruction company. |
| **Q. 241A:**  PS-16.3 | *If the destruction is performed by a third-party destruction company, is it supervised and signed off by two company personnel?* | X |  |  | All assets are destroyed on-site with dual control. Assets are first verified by a Microsoft full-time employee, and then verified by the third-party destruction company. |
| **Q. 241B:**  PS-16.3 | *Does the third party destruction company provide a certificate of destruction for each completed job?* | X |  |  | The third-party provides Microsoft Datacenter Operations with a certificate of destruction, which is verified and stored in Redmond, Washington. |
| **Q. 243:**  PS-17.0, PS-17.3 | *Do you require valid shipping or work order to be created to authorize shipment of client assets out of the facility? If yes, what information does the authorization form capture? (Please specify in the comments box to the right)* |  |  | X | MCIO contracts with specific carriers (FedEx, UPS, DHL) for shipping and receiving physical hardware to datacenters.  Shipping and processing orders are managed by the customer through the Azure Import/Export service in the Azure Management Portal. Work orders are created and managed via a ticketing system. For more information, please see <https://azure.microsoft.com/en-us/documentation/articles/storage-import-export-service/> |
| **Q. 244:**  PS-17.1 | *Do you track and log client asset shipping details?*  *If yes, please provide the details of information logged.*  *(Please specify in the comments box to the right)* |  |  | X | If an asset is shipped, the shipping company selected by the customer assumes the responsibility after handoff of the asset from the datacenter. |
| **Q. 246:**  PS-17.3 | *Do you utilize a courier to transport client assets?*  *If yes, are the following performed or obtained:* |  |  | X | Entrance and exit to secure areas (including areas where information processing and information systems are housed) are protected by the design and implementation of electronic access control systems and mechanisms (such as card key access and/or biometrics technology) to prevent unauthorized access. Additionally, access to secure areas (including those containing information processing and information system facilities) is controlled and isolated from public access areas (such as building lobbies, delivery and loading areas) by electronic access control systems and mechanisms (such as card key and/or biometrics technology) and building design to prevent unauthorized access. |
| **Q. 249:**  PS-17.6 | *Do authorized personnel (e.g., security) observe and monitor the on-site packing and sealing of trailers prior to shipping? If yes, please provide name and title in the comments section.* |  |  | X | Pre-approved deliveries are received in a secure loading bay and are monitored by authorized personnel. Loading bays are physically isolated from information processing facilities. |
| **Q. 252:**  PS-18.0 | *Upon receipt of client assets, do you inspect and compare to shipping documents (e.g., packing slip, manifest log) to ensure that all items were delivered and not damaged?* | X |  |  | Azure Import / Export Services provides a ticketing system to submit physical media for processing at a designated Azure datacenter. |
| **Q. 253:**  PS-18.1 | *Do you perform the following processes immediately after assets are received:* | X |  |  | Azure Media Services provides a OData style REST API for interacting with the service. One of the primary entities in the system is the Asset entity which is used to hold the media files making up a single media asset. Each media file in the Asset entity has an associated AssetFile entity representing that media file. Both the Asset Entity and the AssetFile Entity have unique ID properties that are generated by Media Services when they are created.  A customer can use the OData interface of Azure Media Services to manage the assets in their account. |
| **Q. 255:**  PS-18.3 | *Do you have a process for receiving overnight deliveries securely?* | X |  |  | Pre-approved deliveries are received in a secure loading bay and are monitored by authorized personnel. Loading bays are physically isolated from information processing facilities. Overnight deliveries that are not pre-planned are not accepted and must return during normal business hours. |
| **Q. 256:**  PS-19.0 | *Do you ship client assets using plain, non-descript labeling?* | X |  |  | Packaging to return client assets such as hard drives via Azure Import / Export is provided by the customer. |
| **Q. 257:**  PS-20.0 | *Do you ship all client assets in closed/sealed containers, in locked containers, shrink wrapped, and also with tamper-evident seals, tapes, packaging, or locks?* |  |  | X | Azure is not a content replication facility. |
| **Q. 258:**  PS-21.0 to PS-21.1 | *Do you ensure that package transportation vehicles are locked at all times and packages are kept out of clear view? Which of the following security features do the vehicles have in place:* | X |  |  | Applies to: segregation from driver cabin, locked and sealed cargo area  Azure contracts with third party carriers. |
| **Q. 259:**  PS-21.2 to PS-21.3 | *For highly sensitive content shipments, do you apply unnumbered seals to cargo doors?* |  |  | X | Customers ingest media files into Assets using one of the various methods discussed in the Uploading Media topic of the [Azure Media Services documentation](https://azure.microsoft.com/en-us/documentation/services/media-services/). It is recommended that customers use the Storage Encryption feature of Azure Media Services to encrypt their media files before uploading them to Azure Blob Storage using the Azure Media Services APIs. This is done in such a way that the key used to encrypt the media files is shared with Azure Media Services in a secure manner.  Once the Asset is created and the media files securely uploaded to Azure Media Services, all of the operations on the content occur under automation from actions initiated by or configured by the account owner. For example, the asset owner could create a Job to encode the Asset into a different media format. Or the asset owner could publish an asset for streaming to end users. Account owners can also query the current state of their assets in the system by getting the list of assets in their account, querying the list of jobs in the account (including the input and output assets), getting the streaming locator and asset delivery policy associated with a given asset (telling if the asset is published for streaming and if dynamic encryption is applied). |
| **Q. 259A:**  PS-21.2 to PS-21.3 | *In addition, do you use security personnel to escort content to high risk areas?* |  | X |  | If a third-party individual is on a visitor request, they will be issued a paper badge and must be escorted throughout the facility. If a third-party individual is given temporary access, their ID badge will only give them access into rooms that they have approved access into. |

# Digital Security

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Control IDs** | **MPAA Guidelines** | **Microsoft Azure Response** | | | |
| **Yes** | **No** | **N/A** | **Notes** |
| **Q. 300:**  DS-1.0 | *Are external networks (Internet, extranets, external partner) segregated from the facility's internal network with a firewall?* | X |  |  | Microsoft Azure implements network access control and segregation through VLAN isolation, ACLs, load balancers and IP filters. External traffic to the customer Virtual Machine(s) is restricted to customer-enabled ports and protocols. Network filtering is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted platform components.  Microsoft Azure uses Network Address Translation (NAT) and network segregation to separate customer traffic from management traffic. Outbound network access is restricted and limited to specific VM instances to support the requested tasks. |
| **Q. 301:**  DS-1.1 | *Are firewall rules reviewed periodically and at least every six months?* | X |  |  | All firewall rules and ACLs are documented and reviewed on at least a quarterly basis. All changes are required to follow the approved firewall rule change control process.  Traffic flow policies are implemented on boundary protection devices that deny traffic by default. These policies are reviewed every month to determine any changes required. |
| **Q. 302:**  DS-1.2 | *Are firewalls configured to deny all protocols by default and enable only specific permitted secure protocols to access the WAN and firewall?* | X |  |  | Azure employs boundary protection devices such as SQL DB Gateways (SQL firewall), content gateways, application firewalls, and denial-of-service safeguards to control communications at external and internal boundaries.  Traffic flow policies are implemented on boundary protection devices that deny traffic by default. These policies are reviewed every month to determine any changes required. |
| **Q. 302A:**  DS-1.2 | *Are unencrypted protocols such as Telnet and FTP turned off or blocked at the firewall?* | X |  |  | Unsecure protocols are blocked by default. All guest / VM ports are disabled by default. Host ports controlled by the Azure Fabric are unreachable by non-infrastructure components. |
| **Q. 303:**  DS-1.6 | *Do you restrict remote management of firewalls from any external interfaces?* | X |  |  | Remote access to the Microsoft Azure environment is enabled only to authorized personnel from predefined networks and boundary devices (e.g., Microsoft Azure load balancers) that implement multifactor authentication. Remote access sessions are continuously monitored using automated mechanisms that provide alerts on specific security events. |
| **Q. 304:**  DS-1.3 | *Do you place externally accessible servers (i.e., web server) on the DMZ?* |  |  |  | As a cloud platform service, Azure does not use a DMZ. |
| **Q. 304A:**  DS-1.3 | *Do firewall rules prevent access to internal networks from the DMZ?* |  |  |  | As a cloud platform service, Azure does not use a DMZ. |
| **Q. 305:**  DS-1.4 | *Do you have a patch management program to ensure that systems are up-to-date on patches and maintenance releases?* | X |  |  | Azure component teams receive notifications of potential vulnerabilities and the latest software updates from the Microsoft Security Response Center (MSRC) and MCIO. The component teams analyze software update relevance to the Azure production environment and review the associated vulnerabilities based on their criticality. Software updates are released through the monthly OS release cycle using change and release management procedures. Emergency out-of-band security software updates (0-day & Software Security Incident Response Process - SSIRP updates) are deployed as quickly as possible. If customers use the default "Auto Upgrade" option, software updates will be applied their VMs automatically. Otherwise, customers have the option to upgrade to the latest OS image through the portal. In case of a VM role, customers are responsible for evaluating and updating their VMs. |
| **Q. 305A:**  DS-1.4 | *If you answered, “Yes” to question 305, does this include network infrastructure devices (i.e., routers, switches, firewalls)?* | X |  |  | Please see response to Question 305 above. |
| **Q. 306:**  DS-1.5  DS-6.9  DS-1.12 | *Do you have a process to implement baseline security requirements and configurations for networking and computing equipment including firewalls, routers, switches, servers, workstations, and mobile computing devices?* | X |  |  | Operational Security Assurance (OSA) is a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft, including the Microsoft Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape. OSA combines this knowledge with the experience of running hundreds of thousands of servers in data centers around the world. Microsoft uses OSA to minimize risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are actually being followed effectively. When issues arise, a feedback loop helps ensure that future revisions of OSA contain mitigations to address them.  Microsoft Azure has established baseline configuration standards and procedures are implemented to monitor for compliance against these baseline configuration standards. |
| **Q. 306A:**  DS-1.5  DS-6.9  DS-6.10 | *Have unnecessary services and applications been disabled or removed from content transfer servers?* | X |  |  | MCIO, and consequently Azure, maintains a current, documented and audited inventory of equipment and network components for which it is responsible. MCIO employs automated mechanisms to detect discrepancies of device configuration by comparing them against the defined policies. MCIO turns off the unused ports by default to prevent unauthorized access. |
| **Q. 306B:**  DS-1.5  DS-6.9  DS-6.10 | *Have you developed secure standard builds or images for systems?* | X |  |  | It is a customer responsibility to harden any VM operating systems or templates. Microsoft Azure software and hardware configurations are reviewed at least quarterly to identify and eliminate any unnecessary functions, ports, protocols and services. |
| **Q. 307:**  DS-1.7 | *Do you secure backups of network infrastructure / SAN / NAS devices and servers to a central server on the internal network?* | X |  |  | Backups of key platform components, internal certificates, secrets, user-level information and system documentation are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored for failures and resolved through documented incident handling procedures. Restoration tests are conducted every 6 months. |
| **Q. 308:**  DS-1.8 to DS-1.9  DS-15.9 | *Do you have a vulnerability management process to cyclically identify, classify, remediate, and mitigate security vulnerabilities on networking and computing devices, and applications?* | X |  |  | Microsoft Azure subscribes to MSRC/OSSC monthly patch notifications and scans for vulnerabilities at least quarterly. Identified vulnerabilities are evaluated and remediated per established timeline based on the level of risk.  Vulnerability assessment and scanning tools are specifically designed to operate in virtualized environments. Procedures have been established and implemented to scan for vulnerabilities on MCIO-managed hosts in the scope boundary. MCIO implements vulnerability scanning on server operating systems, databases, and network devices. The vulnerability scans are performed on a quarterly basis at minimum. |
| **Q. 308A:**  DS-1.8 to DS-1.9  DS-15.9 | *How often are internal vulnerabilities scans conducted? What is the interval between tests or vulnerability management cycles? (Please specify in the comments box to the right)* |  |  |  | Microsoft Azure subscribes to MSRC/OSSC monthly patch notifications and scans for vulnerabilities at least quarterly. Identified vulnerabilities are evaluated and remediated per established timeline based on the level of risk.  Vulnerability assessment and scanning tools are specifically designed to operate in virtualized environments. Procedures have been established and implemented to scan for vulnerabilities on MCIO-managed hosts in the scope boundary. MCIO implements vulnerability scanning on server operating systems, databases, and network devices. The vulnerability scans are performed on a quarterly basis at minimum. |
| **Q. 308B:**  DS-1.8 to DS-1.9  DS-15.9 | *How often are external vulnerabilities scans conducted? What is the interval between tests or vulnerability management cycles? (Please specify in the comments box to the right)* |  |  |  | Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure boundary. Red Team exercises are also routinely performed and results used to make security improvements. |
| **Q. 308C:**  DS-1.8 to DS-1.9  DS-15.9 | *How often are internal penetration tests performed by independent third parties? (Please specify in the comments box to the right)* |  |  |  | The Microsoft Azure trustworthy foundation concept ensures application security through a process of continuous security improvement with its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs using both Prevent Breach and Assume Breach security postures.   Prevent Breach works through the use of ongoing threat modeling, code review and security testing. Assume Breach employs Red Team exercises, live site penetration testing and centralized security logging and monitoring to identify and address potential gaps, test security response plans, reduce exposure to attack and reduce access from a compromised system, periodic post-breach assessment and clean state.  Azure validates services using third party penetration testing based upon the Open Web Application Security Project (OWASP) top ten and CREST-certified testers. The outputs of testing are tracked through the risk register, which is audited and reviewed on a regular basis to ensure compliance to Microsoft security practices. |
| **Q. 308D:**  DS-1.8 to DS-1.9  DS-15.9 | *How often are external penetration tests performed by independent third parties? (Please specify in the comments box to the right)* |  |  |  | Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure boundary. Red Team exercises are also routinely performed and results used to make security improvements. |
| **Q. 309:**  DS-1.10 | *Do WAN, extranet, or other site-to-site data circuits utilize private connections and employ encryption of data in transit?* | X |  |  | Customers are accountable for configuring secure private network connections to their Azure subscription environment, such as using IPsec for VPNs and ExpressRoute.  All Azure WAN and site-to-site infrastructure networks are isolated and encrypted using either TLS or IPsec. |
| **Q. 310:**  DS-3.0  DS-14.1 | *Do you segment and isolate networks containing content and production data from other networks (office data, administrative, DMZ, Internet, extranets, etc.)?* | X |  |  | For the Azure infrastructure, production and non-production are physically and logically separated. Microsoft Azure employs network-based and host-based boundary protection devices such as firewalls, load balancers, IP Filters, and front-end components. These devices use mechanisms such as VLAN isolation, NAT and packet filtering to separate customer traffic from management traffic. |
| **Q. 311:**  DS-2.1 | *Have you implemented e-mail content filtering to block malicious software and program types, identify potential phishing e-mails and spam, block e-mails from blacklisted domains, and restrict file sizes?* | X |  |  | Applies to: blocks malicious software, identifies phishing e-mails and spam, blocks e-mails from blacklisted domains, restricts file sizes  Microsoft corporate email systems are protected by anti-malware / anti-spam solutions, and constantly updates signatures and profiles based on CERT and MSRC information.  Customers can use Office 365 for email with their Azure subscription, which also offers anti-malware / anti-spam capabilities. If customers deploy their own email solution within Azure, they should both configure the native anti-virus / anti-malware service for their virtual machines, and/or utilize a third-party security solution for their email and file storage. These are available through the Azure Portal and Application Gallery. |
| **Q. 312**  DS-2.2 | *Have you implemented content and network traffic filtering to block pirate sites, peer to peer traffic, file sharing and storage hubs?* | X |  |  | By default, all network traffic to newly provisioned VMs is blocked by the hypervisor and host firewall. Customers must explicitly configure their Virtual Network to allow Internet or local traffic by creating endpoint mappings.  Customers should additionally configure network and application layer firewalls within their hosted Azure environment to prevent unwanted or unauthorized traffic, such as file sharing sites.  Azure infrastructure does not automatically filter customers' network traffic. Azure's anti-DDOS system helps detect and block known threats and attacks, but customers are responsible for implementing appropriate content controls that meet their business needs. |
| **Q. 313:**  DS-3.2, DS-8.2 | *Do you restrict remote access connections to certain subnets or from networks that contain content data?* | X |  |  | Azure infrastructure and management networks are only accessible from approved Microsoft corporate gateways or secure access workstations.  Customers should configure appropriate access controls within their subscription environment. Azure provides mechanisms for logically segregating traffic on Virtual Networks using firewalls, policies, security groups, and ACLs. |
| **Q. 314:**  DS-3.2 | *Do you employ multi-factor authentication for remote access? (if yes, provide details in the comments box)* | X |  |  | Azure Multi-Factor Authentication (MFA) is available to all Azure customers, and provides token-based authentication using phones or mobile applications.  Microsoft has implemented MFA for all management and support access, including Smartcards, PINs, and phone-based repudiation. |
| **Q. 315:**  DS-3.2 | *Do you review or monitor remote access activity?* | X |  |  | Management or support-level access of Azure's production environment is logged and audited according to the ISMS, and validated through multiple commercial and government audits on an ongoing basis.  Customers should implement identity and access management in their subscription using Azure Active Directory (Azure AD) or other control mechanisms. Azure AD performs logging and reporting for all customer access. |
| **Q. 316:**  DS-3.2 | *Do you maintain an up-to-date list of users authorized for remote access?* | X |  |  | Just-in-time (JIT) access to the Azure customer environment is granted only on an approved and as-needed basis, with only enough privilege to complete the required tasks. Upon resolution, access is revoked; all access is logged.  Customers are responsible for identity and access management within their Azure environment. |
| **Q. 317:**  DS-3.2 | *What security and encryption protocols do you use for remote access?* | X |  |  | IPsec, TLS 1.2, HTTPS  Customers using ExpressRoute to connect their on-premises systems to Azure can use an encrypted VPN session. |
| **Q. 318:**  DS-3.4 to 3.5 | *Do you employ layer 3 switches, strong authentication for management interfaces to switches, and have logging turned on the switches?* | X |  |  | Microsoft Azure controls physical access to diagnostic and configuration ports through physical data center controls. Diagnostic and configuration ports are only accessible by arrangement between service/asset owner and hardware/software support personnel requiring access. Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed. |
| **Q. 319:**  DS-3.4 to 3.5 | *Do you employ hubs or repeaters?* | X |  |  | Microsoft Azure controls physical access to diagnostic and configuration ports through physical data center controls. Diagnostic and configuration ports are only accessible by arrangement between service/asset owner and hardware/software support personnel requiring access. Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed. |
| **Q. 320:**  DS-3.5 | *Do you prohibit dual-homed networking (physical networked bridging) on computer systems within the content/production network?* | X |  |  | For the Azure infrastructure, production and non-production are physically and logically separated. Microsoft Azure employs network-based and host-based boundary protection devices such as firewalls, load balancers, IP filters, and front-end components. These devices use mechanisms such as VLAN isolation, NAT and packet filtering to separate customer traffic from management traffic.  The Microsoft Azure network is segregated to separate customer traffic from management traffic. In addition, the SQL Azure services layer includes TDS gateways that control information flows through stateful inspection. |
| **Q. 321:**  DS-3.6 | *Do you use intrusion detection or prevention systems? (If yes, please describe and specify in the comments box to the right)* | X |  |  | A variety of technical controls are in place to prevent attacks including, but not limited to, Next-Gen firewalls, IDS\APS, network segmentation and network security analytics such as Azure Security Center. |
| **Q. 322:**  DS-3.7 | *Do you use SMTP?* |  | X |  | Customers are not restricted in which protocols they can use in their Azure environment.  However, Azure does not provide email services, and thus does not use SMTP. |
| **Q. 322A:**  DS-3.7 | *If you are using SMTP, are you using SMTP v3 with secure or difficult to guess community strings?* |  |  | X | Please see response to Question #322 above. |
| **Q. 323:**  DS-4.1 to DS-4.2 | *Do you run wireless networks? (If yes, describe the security protocols that are used to secure the wireless networks, in the comments box to the right)* |  | X |  | Azure does not permit or allow wireless connections in the production network environment. Internal security teams regularly scan for rogue wireless signals, and on a quarterly basis rogue signals are investigated and removed. |
| **Q. 323A:**  DS-4.1 to DS-4.2 | *Are wireless networks isolated from networks where content or production work is stored?* |  |  | X | Azure does not permit or allow wireless connections in the Azure production network environment, and does not provide access to customer environments. |
| **Q. 324:**  DS-5.0 | *Do you designate specific systems for loading and extracting data from systems that store content data?* |  |  | X | Datacenter Services Team and Data Center Logistics teams attach the device to the Azure Import/Export servers in the datacenter and notify the requestor. These are specifically designated storage access points. |
| **Q. 324A:**  DS-5.0 | *Do you maintain an access control list with specific source and destinations systems?* |  |  | X | This is a customer control, as content verification should be carried out after migration using Azure Import/Export services. |
| **Q. 325:**  DS-5.1 | *Do you restrict input/output (with the exception of systems used for content I/O) of mass storage, external storage, and mobile storage devices (e.g., USB, FireWire, Thunderbolt, SATA, SCSI, etc.) and optical media burners (e.g., DVD, Blu-Ray, CD, etc.) on all systems that handle or store content?* | X |  |  | Applies to: mass storage, external storage, mobile storage devices, optical media burners  MCIO implements controls on the use of removable media within the Azure in-scope boundaries. Customer content is not accessible via removable media. |
| **Q. 326:**  DS-6.0 to DS-6.4 | *Do you use antivirus, antispam, or endpoint software? (If yes, describe the antivirus programs or systems in place, in the comments box to the right)* | X |  |  | MCIO-managed hosts within the in-scope boundary are scanned to validate anti-virus clients are installed and current signature-definition files exist.  All Azure VMs have Azure Anti-Malware installed by default. (https://azure.microsoft.com/en-us/blog/microsoft-antimalware-for-azure-cloud-services-and-virtual-machines/) Customers may install other anti-virus or intrusion prevention solutions as-needed for their businesses. |
| **Q. 327:**  DS-6.5 | *Do you restrict users from having local administrative rights on their machines, unless industry software requires local administrative rights to run the software?* | X |  |  | Customers are responsible for ensuring the security of their endpoints used to access Azure.  However, all systems used to manage or access the Azure test or production environments have been hardened according to industry best-practices (http://download.microsoft.com/download/7/0/E/70E3858E-8764-4233-A00F-49A3C6C3143C/Security\_Management\_in\_Microsoft\_Azure-11062014.pdf), and have restricted access policies to prevent unauthorized use. |
| **Q. 329:**  DS-6.7 | *Do you require devices that handle content to encrypt the data? (If yes, please provide details in the comments box)* | X |  |  | Customers are responsible for encrypting their VMs or client devices that access their Azure environment.  All Microsoft development and management systems that access Azure infrastructure are encrypted using BitLocker AES-256. |
| **Q. 329A:**  DS-6.7 | *In addition, do you have remote-kill software to perform remote wiping of data on devices?* | X |  |  | Microsoft uses Active Directory Group Policies to manage all connected developer or support systems, in addition to the secure configurations mentioned in item 327 above. Microsoft System Center provides the ability to remotely manage and re-image client machines as-needed.  However, customer data is never stored on local devices, including workstations, removable media, or local hard drives. The customer is responsible for the deletion of data in their Azure Storage account. |
| **Q. 330:**  DS-6.8 | *Do you restrict users from installing unapproved software on computers?* | X |  |  | Microsoft uses Active Directory Group Policies and AppLocker to prevent the installation of unauthorized software on endpoints that access build, test, or production Azure resources.  Customers are responsible for enacting sufficient controls and policies on their endpoints and VMs used within or in conjunction with their Azure environment to prevent unwanted software installation. |
| **Q. 330A:**  DS-6.8 | *How often are systems scanned for an inventory of installed applications? (Please specify in the comments box to the right)* | X |  |  | Azure conducts quarterly patch and vulnerability scans. Applications cannot be deployed directly to the Hypervisor, Host, or Host OS.  Customers should implement appropriate inventory scanning of their virtual machines using suitable mechanisms, and enable system lockdown using tools such as AppLocker to prevent unauthorized software installation. |
| **Q. 331:**  DS-6.11 | *How often is the inventory of computers and system components updated? (Please specify in the comments box to the right)* | X |  |  | The inventory of virtual and physical assets is generated and reviewed on a periodic basis using a combination of information systems, tagging, and Microsoft asset management systems. The generation and audit period varies depending on inventory certification scope (i.e. quarterly, monthly, or other). |
| **Q. 332:**  DS-6.12 | *Do you maintain network topology diagrams?* | X |  |  | MCIO maintains a complete topology view of all datacenter classes, including physical and VLANs, TORs, clusters, network devices, rules, WAN links, and other details. |
| **Q. 332A:**  DS-6.12 | *If there been any significant changes made to the network infrastructure recently, is the documentation up to date?* | X |  |  | Network diagrams are kept up to date as part of the ongoing compliance programs including SOC, ISO, PCI, and FedRAMP. |
| **Q. 333:**  DS-7.0 | *Do you have policies and procedures for managing of user, administrator, and service accounts?* | X |  |  | Azure enforces existing ISMS policies regarding FTE and contractor access to the Azure system components, verification of access control effectiveness, providing JIT administrative access and revoking access when no longer needed, and ensuring staff accessing the Azure platform environment have a business need.  The Information Security Policy requires that access to Azure assets be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews.  Azure uses Active Directory (AD) to manage user accounts. Security group membership must be approved by the designated security group owners within Azure. Automated procedures are in place to disable AD accounts upon the user's leave date. Domain-level user accounts are disabled after 90 days of inactivity. |
| **Q. 334:**  DS-7.1 | *Do you retain evidence of management approvals and associated actions for all account management activities, where possible?* | X |  |  | Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally. MCIO restricts access to audit logs to authorized personnel based on job responsibilities. Event logs are archived on secure archival infrastructure and are retained for 180 days.  Microsoft Azure Fabric Controlled Hardware Device Authentication maintains the credentials used to authenticate itself to various Microsoft Azure hardware devices under its control. The system used for transporting, persisting, and using these credentials is designed to make it unnecessary for Microsoft Azure developers, administrators, and backup services/personnel to be exposed to secret information. |
| **Q. 335:**  DS-7.2 | *Do you assign credentials on a need-to-know / least privilege basis for the following systems, at a minimum:* | X |  |  | Applies to: production systems, network devices, logging systems, client web portal, account management systems, remote access, other (please specify below)  Microsoft Azure enforces the concept of least-privilege and restricts access to information systems including the hypervisor or hypervisor management plane using role-based security groups and two-factor authentication. |
| **Q. 336:**  DS-7.3 | *Do you have a process to rename administrator user IDs and change the password of default accounts?* | X |  |  | Azure uses Active Directory (AD) to manage user accounts. Security group membership must be approved by the designated security group owners within Azure. Automated procedures are in place to disable AD accounts upon the user's leave date. Domain-level user accounts are disabled after 90 days of inactivity.  The Information Security Policy requires that access to Azure assets be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Managers and owners of applications and data are responsible for reviewing who has access on a periodic basis.   A quarterly review is performed by FTE managers to validate the appropriateness of access to MCIO-managed network devices. A quarterly review is performed by FTE managers and MCIO security group owners to validate the appropriateness of user access.  Azure Active Directory password policy requirements are enforced on new passwords supplied by customers within the portal. Customer initiated self-service password changes require validation of older password. Administrator reset passwords are required to be changed upon subsequent login. |
| **Q. 336A:**  DS-7.3 | *Do you limit the use of generic system administrator accounts (e.g. root, administrator) to only special situations which require the use of these accounts?* | X |  |  | Utility programs and the release management process are restricted to authorized personnel only.   Administrative access and privileges to the Azure platform are restricted to authorized personnel through designated AD security groups based on job responsibilities.  Security group membership must be approved by the designated security group owners within Azure. |
| **Q. 337:**  DS-7.4 | *Do you restrict users from being able to grant themselves access to information systems?* | X |  |  | Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Microsoft Azures’ assets is granted based upon business requirements and with the asset owner’s authorization. Additionally:   * Access to assets is granted based upon need-to-know and least-privilege principles. * Where feasible, role-based access controls are used to allocate logical access to a specific job function or area of responsibility, rather than to an individual. * Physical and logical access control policies are consistent with standards. |
| **Q. 337A:**  DS-7.4 | *Is there an independent team responsible for granting access to users?* | X |  |  | MCIO enforces segregation of duties through user defined groups to minimize the risk of unintentional or unauthorized access or change to production systems. Information system access is restricted based on the user's job responsibilities. Documentation on how Microsoft Azure maintains segregation of duties is included in the available security framework audit results on the Azure Trust Center website. |
| **Q. 338:**  DS-7.5 | *Do you log administrator and service account activities?* | X |  |  | Logging and monitoring access is highly restricted to only authorized staff with a business need to access such systems. Microsoft Azure platform components (including OS, CloudNet, Fabric, etc.) are configured to log and collect security events. |
| **Q. 339:**  DS-7.6 | *Do you remove access for users who no longer need access to systems because of the completion of a project, change in job role, or termination? In addition, do you perform the following:* | X |  |  | Applies to: review dormant accounts and disable or remove such accounts, review client web portals or content transfer systems for dormant accounts and disable or remove such accounts  The Information Security Policy requires that access to Microsoft Azure assets to be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Managers and owners of applications and data are responsible for reviewing who has access on a periodic basis.  Privileged accounts are reviewed at least every three (3) months to ensure the privileged access level is still appropriate. Access is modified based on the results of the reviews.  A quarterly review is performed by FTE managers to validate the appropriateness of access to MCIO-managed network devices. A quarterly review is performed by FTE managers and MCIO security group owners to validate the appropriateness of user access.  Security group memberships are reviewed for appropriateness on a quarterly basis and access is modified based on the results of the review. |
| **Q. 340:**  DS-7.8 | *Do you remove local accounts on systems that handle content, where technically feasible?* | X |  |  | Customers are responsible for ensuring least-access for the virtual machines in their Azure environment.  For all infrastructure virtual machines (Host), Azure OS images default to a least-access state. Host OS configurations are hardened according to industry best practices. |
| **Q. 340A:**  DS-7.8 | *If local accounts are used, do you change the default user names and passwords?* |  |  | X | Local accounts are disabled by default per security and hardening best-practices. |
| **Q. 340B:**  DS-7.8 | *Do you restrict remote (over network) use of local accounts?* | X |  |  | Infrastructure servers (Hosts, Host OS) do not support local logon. Virtual Machines are provisioned in a least-access state. Administration is conducted using centrally managed AD domain accounts and security groups.  Management access to host servers is restricted to special-purpose secure gateways and secure access workstations running hardened configurations. |
| **Q. 341:**  DS-8.0 | *Do you require users to create unique usernames and passwords for all systems and applications?* | X |  |  | Users are assigned unique user identifiers in AD based on HR employee IDs after appropriate management authorization. |
| **Q. 342:**  DS-8.1 | *Do you have a strong password policy for all information systems?* | X |  |  | Applies to: minimum password length of 8 characters, minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters, maximum password age of 90 days, minimum password age of 1 day, maximum invalid logon attempts of between 3 and 5 attempts, user accounts locked after invalid logon attempts must be manually unlocked, and should not automatically unlock after a certain amount of time has passed, password history of ten previous passwords |
| **Q. 342A:**  DS-8.1 | *Are there any systems that do not meet the above password requirements? (Please specify in the comments box to the right)* |  | X |  | Password policies are enforced via Active Directory Group Policies, and are applied on a worldwide basis. |
| **Q. 343:**  DS-8.3 | *Have you implemented password-protected screensavers or screen-lock software for servers and workstations?* | X |  |  | Physical / infrastructure servers (hosts) are headless and do not support local logon. Remote configuration of hardware is managed by the Azure Fabric Controllers.  Workstations used to manage Azure Production infrastructure follow industry best-practices for operating system hardening, application control, and AD group policy enforcement for secure configuration. [see <http://download.microsoft.com/download/7/0/E/70E3858E-8764-4233-A00F-49A3C6C3143C/Security_Management_in_Microsoft_Azure-11062014.pdf>] |
| **Q. 344:**  DS-8.4 | *Do you have a layered authentication strategy (multi-factor authentication, identity and access management system, single sign on system, identity federation standards) for WAN and LAN / Internal Network access?* | X |  |  | Azure provides multiple levels of network segregation and authentication for access control. Customers are responsible for configuring access control and security for their Virtual Network deployments.  Each Azure cluster is logically segregated using several VLANs to separate customer traffic from the rest of the Azure network. |
| **Q. 345:**  DS-9.0 | *Have you implemented logging for security events?  If yes, please describe what systems and what kinds of events are logged? (Please specify in the comments box to the right)* | X |  |  | Microsoft Azure Diagnostics enables collection of diagnostic data from an application running in Microsoft Azure. Diagnostic data may be used for debugging and troubleshooting, measuring performance, monitoring resource usage, traffic analysis and capacity planning, and auditing. After the diagnostic data is collected it can be transferred to a Microsoft Azure storage account for persistence. Transfers can either be scheduled or on-demand. Azure Diagnostics is configured using an XML configuration file.   The Azure Threat Management Team utilizes a variety of tools to monitor system events. Azure Access Control Service (ACS) is used to retrieve Windows security event logs from:   * IaaS servers * Domain controllers in the MCIO-Managed domains supporting the IaaS Security Authorization boundary.   Microsoft Azure platform components (including OS, CloudNet, Fabric, etc.) are configured to log and collect security events. Administrator activity in the Microsoft Azure platform is logged. The customer is also responsible for performing these duties and for ensuring secure transport of audit logs.  The customer is responsible for establishing proper log settings. |
| **Q. 346:**  DS-9.1 | *Do you have a centralized log aggregation system?* | X |  |  | Azure systems and services have implemented audit logging and monitoring to capture user activities, exceptions, faults, security events, etc.  The Monitoring and Diagnostics Service (MDS) within Microsoft Azure platform provides automated logging, alerting, and log storage capabilities for monitoring system use and detection of potential unauthorized activity. The primary functions of MDS are:   * **Data Collection** -- Collect event data as per each component team’s specifications on different nodes (VM, Native, and Physical Roles) within Microsoft Azure. * **Data Aggregation** -- Filter and aggregate data events residing on Microsoft Azure nodes into a central repository as per specification provided by component teams. * **Data Analysis** -- Enable queries on structured event data for analysis. * **Information Access** -- Provide interactive and programmatic access to raw and processed data through MDS portal and MDS APIs respectively. |
| **Q. 346A:**  DS-1.11 | *Do your systems use a synchronized time service protocol to ensure they have a common time reference?* | X |  |  | Azure has established procedures to synchronize servers and network devices in the Azure environment with NTP Stratum 1 time servers that sync off of Global Positioning System (GPS) satellites. The synchronization is performed automatically every five minutes. |
| **Q. 347:**  DS-9.4 | *Do you review logs on periodic basis?  If yes, please describe what logs and how often (e.g., daily, weekly) each log is reviewed? (Please specify in the comments box to the right)* | X |  |  | Azure systems are continuously monitored using a combination of automated mechanisms, and logs are periodically reviewed according to ISMS requirements. |
| **Q. 348:**  DS-9.2 | *Do the logging or IDS systems provide alerts based on certain activity in real time, with notifications to investigative personnel? If yes, what types of activity and at what thresholds are notifications sent? (Please specify in the comments box to the right)* | X |  |  | Microsoft Azure Security Monitoring (ASM) leverages the MDS infrastructure to provide logging and alerting upon detection of breaches or attempts to breach Microsoft Azure platform trust boundaries. ASM is implemented as an extension of the Monitoring Agent and is configured to send security-related events to the configured component team’s Storage Account. ASM runs periodic checks based on running processes and key system aspects and uses them to identify deviations that may represent an anomaly.   ASM monitors a number of key security parameters to identify potentially malicious activity on Microsoft Azure nodes such as:   * Unexpected change in firewall settings on a platform service node * Unexpected processes executing on a platform service node * Unexpected drivers installed on root partition or platform service node * Unexpected user account creation or logon sessions * Unexpected group creation   Although ASM monitors for the above security parameters, alerts are generated only for the following:   * Unexpected drivers installed on root partition or platform service node * Unexpected user account creation * Unexpected group creation   The Microsoft Azure Security Group manages response to malicious events, including escalating and engaging specialized support groups. The event and warning logs are examined for anomalous behavior either through an automated alert system or manually when necessary and appropriate actions are taken in accordance with troubleshooting guides. |
| **Q. 349:**  DS-9.8 | *Do you log key and vendor management events and ensure that all keys and certificates are traceable to a unique user?* | X |  |  | Microsoft has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission for the key components of the Azure service. Azure provides each subscription with an associated logical certificate store that enables automatic deployment of service-specific certificates, and to which customers can upload their own (such as Azure Key Vault).   Certificates used in Azure are x.509 v3 certificates and can be signed by another trusted certificate or they can be self-signed. The certificate store is independent of any hosted service, so it can store certificates regardless of whether they are currently being used by any of those services. These certificates and other credentials uploaded to Azure are stored in encrypted form. |
| **Q. 350:**  DS-9.5 | *Do you review logs of internal and external content movement and transfers? If yes, what information is logged? (Please specify in the comments box to the right)* |  |  | X | Azure provides mechanisms for customers to track information transfers, but does not track customer information per ISO 27018 privacy policies.  Internally, Microsoft tracks data flows and network connectivity among its facilities worldwide. Microsoft will not transfer Customer Data outside the geo(s) customer specifies (for example, from Europe to U.S. or from U.S. to Asia) except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where customer configures the account to enable such transfer of Customer Data, including through the use of:   * Features that do not enable geo selection such as Content Delivery Network (CDN) that provides a global caching service; * Web and Worker Roles, which backup software deployment packages to the United States regardless of deployment geo; * Preview, beta, or other pre-release features that may store or transfer Customer Data to the United States regardless of deployment geo; * Azure Active Directory (except for Access Control), which may store Active Directory Data globally except for the United States (where Active Directory Data remains in the United States) and Europe (where Active Directory Data is in Europe and the United States); * Azure Multi-Factor Authentication, which stores authentication data in the United States; * Azure RemoteApp, which may store end user names and device IP addresses globally, depending on where the end user accesses the service. |
| **Q. 351:**  DS-9.6 to DS-9.7 | *Do you restrict logs to appropriate personnel and retain logs for at least one year?* | X |  |  | For services using MDS for logging, the log events are generated on various nodes and are transmitted to MDS for storage and retention. The following mechanisms are used to protect log information in transit and at rest.   * Nodes – Event log information on the Virtual Machines (VMs) can only be accessed through login to the respective VMs. Access to VMs is controlled through an approval process as detailed in the Access Control procedure. * Transmission – The transfer of event log information to Storage is over an HTTPS connection. * Storage – Read-only access to event logs in Component team Storage accounts for Microsoft Azure users is enabled through the MDS frontend portal. The access is restricted through security groups.   For services using MDS, the log configuration adheres to the Microsoft Online Services Record Retention Procedures. Log files containing Customer’s End User Identifiable Information (EII) are classified as MBI and are stored for a minimum period of 90 days after the data is generated by the Azure service. |
| **Q. 352A:**  DS-10.0 to DS-10.2 | *Do policies address the following:* | X |  |  | Applies to: standard devices, BYOD, proper use, antimalware, allowed applications, mobile device management  Mobile devices are not permitted within Azure production datacenters where customer data is stored; wireless networking is not enabled. |
| **Q. 353:**  DS-10.3 to DS-10.9 | *Do you have mobile device management to enforce security controls on mobile computing devices?*  *If yes, do mobile security controls address the following:* | X |  |  | For devices on Microsoft's corporate network only.  Mobile / wireless devices are not allowed to connect to production datacenter infrastructure.  Applies to: encryption, remote wipe, secure backups, inactivity lock, password / PIN, antimalware, anti-rooting |
| **Q. 355:**  DS-11.1 | *Do you encrypt content data on hard drives? If yes, how and what kind of encryption? (file and folder, partition, full disk, AES128, AES256, etc.) (Please specify in the comments box to the right)* | X |  |  | Microsoft Azure does not automatically encrypt tenant data in storage. However, there are tools within Azure and third-party tools that allow encryption of data in Azure storage. Customers may implement encryption at-rest using .NET cryptographic services.   For customers using Virtual Machines, additional options are available, including the Encrypting File System in Windows Server 2008 R2 (and above), Azure Rights Management Services, as well as Transparent Data Encryption (TDE) in SQL Server 2008 R2 (and above).   Azure supports strong cryptography using standard, validated formats including AES-256, IPsec, 1024-bit Perfect Forward Secrecy (PFS) and FIPS-140-2. Azure allows a customer manage their own keys using independent Azure services for key vaulting, off-cloud third party key vaulting, or their own off-premises key management solution.  More information on available options can be found in the Data Protection whitepaper at: <http://go.microsoft.com/fwlink/?linkid=398382&clcid=0x409> |
| **Q. 356:**  DS-11.2 | *Do you send decryption keys using an out-of-band communication protocol (i.e., not through the same channels as the content itself)?* | X |  |  | Through the use of Azure Key Vault, Azure provides a service for customers to manage and safeguard their cryptographic keys used by cloud applications. Key Vault encrypts keys and secrets, such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords, by using keys that are protected by hardware security modules (HSMs). HSMs are certified to FIPS 140-2 level 2. |
| **Q. 357:**  DS-11.3 | *Do you have policies and procedures for key management?* | X |  |  | Azure has documented and communicated Standard Operating Procedures (SOPs) that provide implementation guidance to operational teams. The SOPs provide documentation establishing and defining Azure encryption management policies, procedures and guidelines, are published at designated internal locations, and are reviewed annually.  Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. Additional information may be obtained through the Customer's Account Manager. |
| **Q. 358:**  DS-11.5 | *Do you store private or secret keys securely (e.g., with a separately stored key-encrypting key, within a secure cryptographic device, etc.)?* | X |  |  | The customer is responsible for this control. Through the use of Key Vault, Azure provides a service for customers to manage and safeguard their cryptographic keys used by cloud applications. Key Vault encrypts keys and secrets, such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords, by using keys that are protected by hardware security modules (HSMs). HSMs are certified to FIPS 140-2 level 2. |
| **Q. 361:**  DS-12.0 to DS-12.2 | *Do you maintain detailed tracking of access to digital content? If yes, what log information is logged? How often are the logs reviewed? What is the retention period of the logs? (Please specify in the comments box to the right)* |  |  | X | This is a customer control. Azure provides mechanisms enabling customers to track information access and usage, but does not do so on behalf of customers. |
| **Q. 363:**  DS-13.0 | *Do your content transfer systems employ strong encryption (e.g., AES128, AES256 or better)?* | X |  |  | Customers may configure Azure to enable encryption-in-transit by configuring HTTPS endpoints. Customers using Virtual Machines who wish to encrypt traffic between Web clients and Web servers in their VMs can implement TLS. Other enhancements to network traffic security include using IPsec VPNs or ExpressRoute to encrypt direct communications between the customer’s datacenter and Microsoft Azure.   For Azure SQL Database, all communication to and from SQL Database requires encryption (TLS 1.1) at all times. For customers who are connecting with a client that does not validate certificates upon connection, the connection to SQL Database is susceptible to "man in the middle" attacks. It is the customer’s responsibility to determine if they are susceptible to this type of attack. Certificates must use a minimum of 2048-bit encryption. |
| **Q. 364:**  DS-13.0 | *Do you restrict access to content transfer systems to only authorized users?* |  |  | X | This is a customer control.  Azure has established and implemented procedures to enforce segregation of key management and key usage duties. Azure key management encompasses the entire life cycle of cryptographic keys and has identified a method for establishing and managing keys in each management phase from generation, installation, storage, rotation and destruction. |
| **Q. 365:**  DS-13.1 | *Do you have an exception and client sign-off process if insecure transfer methods or systems are used?* |  |  | X | This is a customer control. Azure provides mechanisms enabling customers to track information access and usage, but does not do so on behalf of customers. |
| **Q. 366:**  DS-14.0 | *Do you use dedicated servers or systems (not running other applications, services, or software) for content transfers?* |  |  | X | Azure Import / Export services run in dedicated Virtual Machines. |
| **Q. 367:**  DS-14.2, DS-15.3 | *Do you place web portal and content transfer servers in a DMZ, separated from the content data or production network?* |  |  | X | Transactions involving the Microsoft Azure Portal, including purchase of services, is encrypted using TLS 1.2 256-bit encryption. SSL/TLS is mandatory when accessing the Azure Portal or System Management API (SMAPI). Microsoft Azure complies with PCI-DSS standards and completes an annual PCI audit by an independent, 3rd party PCI-DSS Qualified Security Assessor company. |
| **Q. 367A:**  DS-14.2, DS-15.3 | *Do you use ACLs to restrict data traffic to and from the DMZ?* |  |  | X | Azure customers are entirely responsible for protection and encryption of their e-commerce transactions, however, Azure ensures critical communications such as calls to the API or intra- Azure communication are encrypted, authenticated, and integrity controlled via protocols such as SSL. Customers can optionally configure SSL/TLS for defense-in-depth on their Virtual Networks.   Storage REST APIs over HTTPS can also be used to interact with Azure Storage and SQL Database. When populating data into SQL Database, you can encrypt information before it is copied over. Note that data only remains encrypted until it is used and placed in memory on the SQL Database compute node, at which point it exists in an unencrypted state. |
| **Q. 368:**  DS-14.3 to DS-14.4 | *Do you have a process to remove content from content transfer devices/systems immediately after successful transmission or receipt?* |  |  | X | Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that can’t be wiped we use a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. All Microsoft Azure services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle. |
| **Q. 368A:**  DS-14.3 to DS-14.4 | *Are automatic notifications sent to production coordinators upon outbound content transmissions?* |  |  | X | This is a customer responsibility. DRM and DLP tools are available from Microsoft and third parties to implement content tracking, but Azure does not provide these by default.  Content access can be logged using Azure monitoring systems. |
| **Q. 369:**  DS-15.7 | *Do you set access to content on internal or external portals to expire automatically at predefined intervals?* |  |  | X | This is a customer responsibility. Azure does not control access to customer content stored in a subscription.  Content policies should be managed according to the customer's ISMS. |
| **Q. 370:**  DS-15.2 | *Do you have a process to review file and directory permissions at least quarterly to ensure that access is restricted to only those that require it?* | X |  |  | Microsoft does not maintain any standing access to customer data or resources.  Azure employs a defense in depth strategy for boundary protection, including secure segmentation of network environments through several methods including VLAN segmentation, ACL restrictions and encrypted communications for remote connectivity.  Azure has a suite of controls around according to the Principle of least privileges - Appropriateness of access at the datacenters is made by the datacenter management and verified during the quarterly access review process:   * Allocation and use of privileges * User registration * Quarterly physical access review * User registration & termination * Visitor access * Segregation of duties |
| **Q. 371:**  DS-15.4 | *Have you implemented multi-factor authentication for the following systems* | X |  |  | Applies to: client web portal, content transfer systems, key generation, e-mail, remote access, other (please specify below)  Any service or application within Azure can be enabled with Azure Multifactor Authentication (MFA), which provides additional mechanisms for identity verification and monitoring through Active Directory. |
| **Q. 372:**  DS-15.5 | *Do web portals employ HTTPS?* | X |  |  | Customers may configure Azure to enable encryption-in-transit to the Azure Management Portal by configuring HTTPS endpoints. Microsoft Azure requires TLS encryption by default and does not store passwords or credentials in plaintext. |
| **Q. 373:**  DS-15.6 | *Do web portals avoid the use of persistent cookies or cookies that store credentials in plaintext?* | X |  |  | The Microsoft Azure trustworthy foundation concept ensures application security through a process of continuous security improvement with its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs using both Prevent Breach and Assume Breach security postures. This methodology is applied across all Azure systems and tools, including customer interfaces and portals.  Prevent Breach works through the use of ongoing threat modeling, code review and security testing; Assume Breach employs Red Team exercises, live site penetration testing and centralized security logging and monitoring to identify and address potential gaps, test security response plans, reduce exposure to attack and reduce access from a compromised system, periodic post-breach assessment and clean state.  Azure validates services using third party penetration testing based upon the OWASP top-ten and CREST-certified testers. The outputs of testing are tracked through the risk register, which is audited and reviewed on a regular basis to ensure compliance to Microsoft security practices. |
| **Q. 374:**  DS-15.11 | *Do you have an e-mail encryption system, i.e. secure e-mail application or service to encrypt sensitive data in e-mails or attachments?* | X |  |  | Microsoft corporate email used by Azure support and engineering staff provides encryption and rights management, as well as Active Directory-based access controls and policies. This system is separate from Azure production infrastructure, and is not used for the transfer of customer data.  Customers may elect to implement their own encryption and rights management solution using Exchange Server, Exchange Online, Office 365, or other communications platform to work with their Azure environment. Office 365 provides content encryption, data protection, monitoring, and Azure AD-based access controls and reporting for email and documents. |

# References and Further Reading

The following resources are available to provide more general information about Microsoft Azure and related Microsoft services, as well as specific items referenced in the main text:

* Microsoft Azure Home – general information and links about Microsoft Azure
  + <http://azure.microsoft.com>
* Microsoft Azure Developer Center – developer guidance and information
  + <http://msdn.microsoft.com/en-us/azure/default.aspx>
* Security Best Practices For Developing Microsoft Azure Applications (white paper)
  + <http://download.microsoft.com/download/7/3/E/73E4EE93-559F-4D0F-A6FC-7FEC5F1542D1/SecurityBestPracticesWindowsAzureApps.docx>
* Microsoft’s Security Development Lifecycle (SDL)
  + <http://www.microsoft.com/security/sdl/>
* Microsoft Cloud Infrastructure and Operations group
  + <http://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx>
* Microsoft Security Response Center [where Microsoft security vulnerabilities, including issues with Microsoft Azure, can be reported]
  + <http://www.microsoft.com/security/msrc/default.aspx>
  + Or via email to [secure@microsoft.com](mailto:secure@microsoft.com).
* Service Trust Portal
  + <https://www.microsoft.com/en-us/TrustCenter/STP/default.aspx>