|  |  |  |
| --- | --- | --- |
| Azure Blueprint | | |
| DFARS Customer Responsibility Matrix This document identifies Microsoft Azure Government’s compliance status for Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 requirements. This document further identifies customer responsibilities for enabling implementation of DFARS requirements in Azure Government. Azure Government customers may have several options for making DFARS 252.204-7012 commitments.  These could include NIST SP 800-171 compliance, FedRAMP Moderate, FedRAMP High, or other comparable programs. Microsoft Azure Government can accept required DFARS flow downs when applicable, and provides the following compliance Blueprint programs: FedRAMP Moderate, FedRAMP HIGH, DoD SRG L4 and L5, and NIST 800-171. These requirements apply to all Defense Industrial Base contractors in order to protect against the loss, misuse, unauthorized access, or modification of covered defense information and the systems that contain that information.    ***Disclaimer:*** *The contents of this document are intended solely for the authorized user and contains confidential and/or privileged information - which is legally protected from disclosure. You are hereby notified that any use, dissemination, altering, copying, or storage of this document is strictly prohibited. This document is developed as a reference and should not be used to define all means by which a customer can meet specific compliance requirements and regulations. Customers should seek legal support from their organization on approved customer implementations.* | | |
| **DFARS requirements**  **252.204-7012** | **Microsoft Azure Compliance Status** | **Customer Responsibility** |
| **Adequate security for external cloud service providers.** | **Microsoft has attained FedRAMP High authorization for Azure Government**. | **Contractor systems could be granted a FedRAMP P-ATO or Agency ATO leveraging the Azure FedRAMP P-ATO.** |
| **Cyber incident reporting requirement** | **Microsoft's** [Online Services Terms](http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31) May 2017 **include security terms that outline our commitment to customers around incident response and incident notification**. Please refer to the relevant Online Services Terms for reference:  Security Incident Notification  If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft’s equipment or in Microsoft’s facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a “Security Incident”), Microsoft will promptly (1) notify Customer of the Security Incident; (2)  investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3)  take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.  Notification(s) of Security Incidents will be delivered to one or more of Customer’s administrators by any means Microsoft selects, including via email. It is Customer’s sole responsibility to ensure Customer’s administrators maintain accurate contact information on each applicable Online Services portal. Microsoft’s obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.  Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.  Incident Response Process  Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.  For each security breach that is a Security Incident, notification by Microsoft (as described in the “Security Incident Notification” section above) will be made without unreasonable delay and, in any event, within 30 calendar days.  Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time."  Microsoft commits to limit access and use of Customer Data in the Online Service terms and through our security processes set forth in the System Security Plan (the basis of our FedRAMP authorization). Microsoft will work with the customer to identify any Customer Data involved in a Security Incident so that the customer can determine if it meets the reporting obligations for Cyber Incidents under the DFARS as part of its commitment to provide customers with detailed information on a Security Incident. Additionally, we will work with customers to help ensure they have relevant information to report via DIBnet. | **Microsoft Azure Government customers should support incident reporting from Microsoft Azure Government as well as to end-customers.**  Notification(s) of Security Incidents will be delivered to one or more of Customer’s administrators by any means Microsoft selects, including via email. It is Customer’s sole responsibility to ensure Customer’s administrators maintain accurate contact information on each applicable Online Services portal. Microsoft’s obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.  Customer will be responsible for notifying Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.  Azure Government customers must determine and provide a means to support cyber incident reporting to end-customers. |
| **Malicious software** | **Microsoft will work with customers to submit malicious software** (i.e., Viruses, malware, rootkits, worms, and scripts) **found in Azure Government assets in connection with a cyber incident to the DoD Cyber Crime Center (DC3).**  PAAS- Azure Government assets are protected from malicious software through the use of anti-malware software in accordance with our FedRAMP authorization. Anti-malware software helps provides both preventive and detective control over malicious software. Anti-malware tools help detect files determined to be malicious and send alerts to Azure Government administrators, which is one way to trigger the incident response process. | **Azure Government customers running IaaS deployments should ensure that Malicious software protections are deployed to systems within the Azure Government customer subscription. Malicious software found in customer Azure Government resources in connection with a cyber incident should be reported to DoD Cyber Crime Center (DC3).**  IAAS - The customer is responsible for employing malicious code protection at information system entry and exit points to detect and eradicate malicious code and use code protection mechanisms to protect assets from malicious software. |
| **Media preservation and protection** | **Microsoft preserves and protects Customer Data in accordance with our FedRAMP System Security Plan and the Online Service Terms.**  Except for free trials, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer’s subscription so that Customer may extract the data.  **Physical or Virtual systems impacted by Security Incidents are treated in accordance with audited FedRAMP incident response processes**  Microsoft commitments regarding Security Incident notification (above) would continue to support preservation and access to preserved forensics. | **Azure Government customers should define customer data preservation and protection terms.**  Except for free trials, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer’s subscription so that Customer may extract the data.  Azure Government customers should determine the data preservation requirements for end-customers and define the necessary agreements for data retention and deletion. |
| **Access to additional information or equipment necessary for forensic analysis** | **Microsoft makes commitment in the Online Services Terms for providing detailed information to customer and DoD upon request.**  Per the Microsoft [Online Services Terms](http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31) May 2017. “If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft’s equipment or in Microsoft’s facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a “Security Incident”), Microsoft will promptly (1) notify Customer of the Security Incident; (2)  investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3)  take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.”  Customer also have access to their own virtual machines in accordance with the data access and preservation commitments described above, which may also support cyber incident forensics investigations.  Azure Government customers have additional rights permitting government access to physical facilities. | **Azure Government customers should support forensic investigations within their cloud systems.**  Customer have access to their own virtual machines in accordance with the data access and preservation commitments described in the Microsoft Online Services Terms, which may support cyber incident forensics investigations.  Customers should determine what additional information can be provided to end-customers to support forensic investigations and provide this information to the end-customer. |
| **Cyber incident damage assessment activities** | **Microsoft will support its customers with the damage assessment activities to investigate the cyber incident**. Audit and monitoring data are retained for at least 90 days in accordance with the FedRAMP System Security Plan. | **Azure Government customers should provide means to support incident investigation and damage assessment activities.** This should include at a minimum retaining the necessary audit and monitoring data necessary to support incident investigation. |

## Revision History

| Date | Description | CRM Version | Author |
| --- | --- | --- | --- |
| 8/2/2017 | Initial Creation | 1.0 | Microsoft |
| 9/28/2017 | Updated for IaaS and PaaS responsibilities as needed. | 2.0 | Microsoft |