**Microsoft Office 365 Security**

Microsoft Office 365 has been implemented at UMB and there have been many questions asked about the security of Office 365 applications.

**For the reasons identified below, it is recommended that personal computer files containing UMB data, including sensitive data, be stored in the Microsoft Office 365 infrastructure.**

Microsoft Office 365 Security Overview

Microsoft Office 365 is a “cloud” based service, which means that UMB data are stored off-campus in the Microsoft server and data storage infrastructure. While some vendor hosted cloud services may have security vulnerabilities, Microsoft Office 365 has very strong IT security and actually offers an enhanced level of security that was not previously available for most UMB data that are stored on the UMB campus. Microsoft Corporation has substantially more resources than UMB and other universities that have implemented Office 365 and can afford teams of security personnel and extensive security technologies for protecting University data.

UMB’s data in the Microsoft Office 365 infrastructure is protected by a variety of technologies and processes, including various forms of encryption. UMB also has a signed Business Associates Agreement (BAA) with Microsoft that effectively addresses all of the security requirements for HIPAA related data. Microsoft services covered under the BAA have undergone audits conducted by accredited independent auditors needed for the Microsoft ISO/IEC 27001 certification.

Microsoft enterprise cloud services also passed all of the security assessments required by the federal government (FedRAMP assessments). Microsoft has been granted authority and certification to store confidential data collected by federal agencies.

The encryption and other security technologies built into Office 365 and managed by Microsoft protect UMB data from a variety of risk scenarios. Multiple layers of security are provided for storing and protecting UMB data in the Microsoft Office 365 cloud infrastructure. The protection of customer content in Microsoft’s cloud services infrastructure is of paramount importance to Microsoft Corporation.

Microsoft Corporation Office 365 Information Security Technologies

For data at rest, Microsoft Office 365 uses volume-level and file-level encryption. For data in-transit, Microsoft Office 365 uses multiple encryption technologies, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec). Cryptographic capabilities are employed to protect the confidentiality, integrity, and availability of data within Office 365. The modules and ciphers used are Federal Information Processing Standards (FIPS 140-2) validated.

The Microsoft Office 365 servers in their Azure infrastructure use a feature called BitLocker to encrypt the disk drives containing log files and customer data at rest at the volume-level. BitLocker encryption is a data protection feature that is built into Windows. BitLocker is one of the technologies used to safeguard against threats in case there are lapses in other processes or controls (e.g., access control or recycling of hardware) that could lead to someone gaining physical access to disks containing customer content. In this case, BitLocker eliminates the potential for data theft or exposure because of lost, stolen, or inappropriately decommissioned computers and disks.

In addition to using volume-level encryption, OneDrive for Business, Skype for Business, and SharePoint Online also use file-level encryption. In Skype for Business, UMB data at rest may be stored in the form of files or presentations that have been uploaded to the Microsoft storage infrastructure by UMB employees. The Web Conferencing server encrypts content using Advanced Encryption Standard (AES) with a 256-bit key.

All customer content in SharePoint Online is protected by unique, per-file keys that are always exclusive to a single Microsoft “tenant”. When a file is uploaded, encryption is performed by SharePoint Online within the context of the upload request, before being sent to Microsoft Azure data storage. When a file is downloaded, SharePoint Online retrieves the encrypted content from Azure storage and decrypts the content before sending it to the user.

In addition to protecting customer content at rest, Office 365 uses encryption technologies to protect UMB content in-transit. Data are in-transit when a client machine communicates with an Office 365 server, or when an Office 365 server communicates with another Office 365 server, or when an Office 365 server communicates with a non-Office 365 server that supports Transport Layer Security (TLS) encryption.

For more information regarding the security of Microsoft Office 365 applications and the UMB IT Security Program, please contact the IT Security & Compliance Office at 6-8337 or

Security-Compliance@umaryland.edu