DCB1596 Conformance Assessment:

Microsoft
Date: 08/11/2022
ICT Service Provider: Microsoft
Date of ICT Service Provider conformance: 12/11/2022

Purpose

This document provides the results of a conformance assessment undertaken by NHS Digital to assist health and care organisations who wish to self-accredit their services to DCB1596 Secure Email. This typically means that this organisation operates its own in-house email service.

Part of this document provides the results of a self-conformance assessment undertaken by Microsoft covering the Health and Care elements of the DCB1596 Secure Email Standard. The ICT Service Provider section covers service controls.

Each organisation must make its own decisions with respect to the standard. The assessment is for a single point in time and does not give secure email connectivity between email systems. This requires connectivity with a secure email gateway or by using secure configuration settings.

Guidance Notes

The conformance statement issued is based on Microsoft's Service assertions, supported by evidence.

The first section of this conformance statement only requires the dates at which each policy related requirement was achieved / published (for example, within the last 6 months) in agreement with their senior management. For the ICT Service Provider section, we require evidence that each requirement is met.

Elements of interest: That clear risk reports are presented, highlighting the residual risks that have been accepted and signed off by senior clinical safety and ICT members of staff in an organisation.

NHS Digital confirms a level of conformance was achieved, has authorised the creation of the email domain and that the evidence presented meets the requirements of the standard, but in no way warranties local compliance. This applies to email usage only and NHS Digital reserves the right to audit any information submitted.

ICT Service Provider

#	Requirement	Statement of Conformance
Information Security		
1	The Service Provider MUST at all times maintain a secure service, even when the service is unavailable to users.	**Met.** Microsoft continually operates the Office 365 service in compliance with all of our security controls, including ISO27001, HIPPA, CJIS, SSAE 16. The service is also maintained to the DCB1596 BCS as required for NHS Secure Email standard. This is assessed annually as part of the Microsoft "continuous compliance" procedures.
2	Each Service Provider MUST maintain an Information Security Management System (ISMS) that conforms to ISO/IEC 27001:2013, based on ISO/IEC 27002:2013 Information technology - Security techniques - code of practice for information security controls or the Data Security and Protection Toolkit (DSPT) in the case of health and social care organisations. ISO/IEC 27001: 2013 conformance may be evidenced by appropriate certification by a United Kingdom Accreditation Service (UKAS[1]) accredited certification organisation, based on a suitably scoped Statement of Applicability relevant to the email service. Internationally operated services may provide certification from a member of the International Accreditation Forum. DSPT submissions will be verified on the DSPT website.	**Met.** The Microsoft Office 365 service maintains an ISMS that is certified to the BS ISO/IEC 27001: 2013
3	If applicable, the information security controls contained within the scope, on which the Service Provider's ISO/IEC 27001:2013 certification or DSPT return is based, MUST be relevant to the email service.	**Met.** The Microsoft Office 365 service information security controls are relevant to the email service as part of DCB1596 Secure Email Standard

[1] https://www.ukas.com/search-accredited-organisations/

	Conformance should be evidenced by the applicable Statement of Applicability (SoA).	
4	The Service Provider MUST maintain an Information Security Policy, as part of its ISMS (conforming to ISO/IEC 27001:2013, ISO/IEC 27002:2013) which sets out the security aims and objectives, as well as security measures to be implemented and maintained. The security policy MUST be regularly reviewed and updated by the Service Provider and MUST be endorsed by the Service Provider's senior management. A copy should be supplied as evidence.	**Met.** The Microsoft Office 365 service maintains a security policy that operates to DCB1596 Secure Email Standard
5	Each Service Provider MUST have a suitably scoped independent IT Health Check (ITHC) / penetration test carried out (by a CHECK / Tiger scheme accredited or CREST member organisation), encompassing the email system and any external network interfaces (including perimeter security / access control devices). Conformance should be evidenced by an ITHC / penetration test report, conducted within the last 12 months, with all identified findings remediated / mitigated and any residual risks accepted by the Senior Information Risk Owner. All risks are expected to be remediated unless there are exceptional reasons not to do so or in the view of NHS Digital is sufficiently mitigated.	**Met.** The Microsoft Office 365 service runs regular penetration tests to DCB1596 Secure Email Standard as detailed at www.microsoft.com/trustcenter It is the responsibility of each Organisation to configure their Microsoft Office 365 instance and independently verify that with an IT Health Check.
6	The email service MUST provide anti-virus, anti-malware and anti-spam filtering, in addition to commodity content management such as attachment blocking, virus / spam filtering capabilities and data leakage prevention, for example, encrypt protectively marked email destined for the internet. The service MUST also provide for the management of spoofed email and items that cannot be checked such as S/MIME encrypted or password protected attachments. The service MUST support Domain Based Message Authentication and	**Met.** Microsoft Office 365 supports anti-virus, anti-malware and anti-spam filtering, including alerting and blocking spoofed / lookalike domains. DMARC, SPF and DKIM. MTA-STS and TLS-RPT are also supported. It is the responsibility of each Organisation to configure Microsoft Office 365 appropriately to comply with this

	Reporting (DMARC) with supporting public Domain Name System (DNS) entries for Sender Policy Framework (SPF) set to quarantine with an agreed timeline to implement a blocking policy **no later than 3 months after accreditation**. All outgoing email MUST be signed with Domain Keys Identified Mail (DKIM). The service SHOULD support MTA-STS, TLS-RPT and use opportunistic Transport Layer Security (TLS) in accordance with National Cyber Security Centre (NCSC) requirements on ciphers and certificates. All outbound connections to the public sector and business partners must use TLS in accordance with National Cyber Security Centre requirements on ciphers and certificates as soon as possible and by no later than **March 2020**. The commissioner of the email service must ensure adequate policies and / or contractual agreements are in place to safe guard this.	Standard: Microsoft Office 365 Configuration Guide TLS connections can be enforced on a per-domain basis to meet the NCSC requirement for secured outbound connections to public sector /business partner organisations. It is the responsibility of each Organisation to configure Microsoft Office 365 with appropriate TLS enforcement.
7	All OFFICIAL data (particularly patient identifiable and OFFICIAL SENSITIVE) MUST be maintained in accordance with the Information Commissioner's Office data protection guidance, paying particular note to Principle 7 and the guidance on the use of cloud computing.	**Met.** The Microsoft Office 365 service operates in accordance with the Information Commissioner's Office data protection guidance and GDPR. It is the responsibility of each Organisation to configure Microsoft Office 365 appropriately  Office 365 GDPR control mapping 5.2
8	The Service Provider MUST provide tools to ensure that mobile devices are appropriately secured when accessing the email service. This SHOULD include: • Functions to allow / deny / quarantine by device type, organisation or groups of users. • Remove device, expire password, and wipe any data associated with the service. • Reporting functions / capabilities.	**Met.** The Microsoft Office 365 Service provides extensive features to allow the policy control of access by mobile devices. The tenant administrator can apply policies to all devices connecting that are in line with the NHS organisations acceptable use policy. These policies can be enforced across all or groups

	• Detect and block rooted (i.e. jail broken) devices.	allowing various levels of control. It is the responsibility of each Organisation to configure Microsoft Office 365 appropriately
9	The Service Provider SHOULD provide eDiscovery tools to support the administration of the service, especially with respect to the EU General Data Protection Regulation, Data Protection Act 2018 and Freedom of Information Act 2000.	**Met.** The Microsoft Office 365 Service provides eDiscovery tools to provide the tenant administrators with the ability to search and filter across all email, in line with the Data Protection and acceptable use statements. Should there be a requirement to retain copies of email customers should purchase the relevant Office 365 licence. It is the responsibility of each Organisation to configure Microsoft Office 365 appropriately
10	Data must only be hosted in locations detailed in the NHS and social care off-shoring policy. Countries where data is hosted to be listed.	**Met.** All Exchange data held within the Microsoft Office 365 Tenant is held within the EEA, (Ireland and the Netherlands) or UK and is dependant on the tenant location. All active directory data is stored within Ireland and the USA. Support centre staff in the USA, Bulgaria and Ireland may have access to customer authored data. Microsoft have asserted sufficient controls are in place to ensure access by support staff is strictly controlled. Health and care organisations must also comply with DSPT requirement which requires organisations undertake an appropriate risk assessment
Safety		
11	The email service MUST comply with the provisions of DCB0129: Clinical Risk	**Met.** Microsoft have a Clinical Safety to Release Certificate

	Management: Its Application in the Manufacture of Health IT Systems.	
Interoperability		
12	Each Service Provider SHOULD comply with the open standards policy.	**Met.** The Microsoft Office 365 service complies with a number of email interoperability standards as detailed in the supporting evidence. For users accessing the service they can access it using web (http) and email client (IMAP, POP, SMTP and LDAP) standard protocols with additional Microsoft proprietary protocols supported for richer functionality/clients. The web interface is WCAG AA compliant.
13	Each service provider MUST enable inbound and outbound opportunistic Transport Layer Security (TLS) version 1.2 or better for secure email transport between other secure email services.	**Met.** The Microsoft Office 365 service provides the tools to meet the DCB1596 Secure Email Standard. It must be noted that the configuration must be completed to be compliant. TLS connections can be enforced on a per-domain basis to meet the NCSC requirement for secured outbound connections to public sector /business partner organisations. It is the responsibility of each Organisation to configure Microsoft Office 365 with appropriate TLS enforcement.
14	TLS Ciphers should conform with current NCSC guidance.	**Met.** The Microsoft Office 365 service provides the tools to meet the DCB1596 Secure Email Standard. It must be noted that the configuration must be completed to be compliant