Document ID	REC042
Document Title	Customer Data Access & Data Security - Microsoft Cloud Support and Services
Author	Nanda Narayanan
Version	3
Classification	Controlled

Revision History		
Date	**Version**	**Change**
13/11/2025	2025111	Document created
01/12/2025	2025122	Document review by Group CISO
02/12/2025	2025123	Reviewed by Kathy Leach and changes accepted – passed to Stephen Crowe (Azure Managed Service) & Matt Bradley (Microsoft Consultancy) to add use cases for managed services and consultancy.

Distribution		
Date	**Version**	**Distribution**
10/12/2025	2025123	Compass – All Staff, Company Website

Signed			
Date	**Version**	**Name**	**Role**
10/10/2025	2025123	Kathy Leach	Head of Support Services

Contents

Introduction

Bytes Software Services (Bytes) prioritise the security and privacy of our customers' data. Our data security policies are designed to protect sensitive data and ensure compliance with recognised industry standards, including ISO 27001. To maintain confidentiality and integrity, we have implemented robust security processes and controls that uphold the highest standards of protection.

Scope

The purpose of this document is to detail the extent to which the Bytes Software Services Microsoft Cloud Support Team can access Customer Environments as part of their responsibilities as a Microsoft Cloud Support Provider, and to document the controls Bytes have in place to prevent any unauthorised access.

This specifically relates to Bytes access to customer environments through Microsoft Partner Center and Azure Lighthouse. Both systems are provided, supported and maintained by Microsoft, but our use of them allows access to your data and information under specific circumstances. It is therefore important that we explain what these are, and how we secure that access appropriately as part of your supply chain security.

Why we need access

There are some fundamental reasons why we need access in this manner and these are:

1. Creation of support cases with Microsoft on your behalf. You cannot raise these directly and a partner (in this case Bytes) needs to raise these on your behalf.
2. To be able to provision licenses into your tenant that you have purchased and where required to manage your license counts and grants with Microsoft.
3. To be able to provide support under your support contracts that you hold with Bytes.
4. Onboarding to the Azure Managed Service requires Guest access.
5. To be able to make changes and perform deployments under the Azure Managed Service.

It is important to ensure that you understand the key principles that we apply to this access, as well as the steps we recommend that you take, and the control that you have. Please see the following sections.

Key Principles

- Customer data always remains the property of the Customer.
- Bytes only accesses data with prior written authorisation and for the minimum time required.

- All access is logged and monitored using Microsoft's native audit tools, and we can assist you with the configuration of this to provide transparency of our operations.
- Bytes enforce strong security measures such as phishing resistant MFA, encryption, endpoint protection, and regular compliance training, as well as many more controls.
- All access is performed using Bytes-managed devices and secure environments.
- Administrative roles are granted only when necessary.

Customer Recommendations

- We would recommend that you implement AES 256-bit encryption for all stored data in Azure, Microsoft Lockbox in M365 if you have E5 licenses and BYOK (Bring Your Own Key) for data encryption in D365 – as this reduces both Microsoft and any partners from viewing data in your solution.
- We would recommend that you include our access within the audit logs to ensure that you have visibility of our access. Our team can show you how to set this up within your tenants.
- We recommend you configure alerts for our access, so that you are notified when we access your systems so you can ensure that we have a reason for this access. Our team can show you how to set this up within your tenants.
- Conduct periodic reviews to ensure that you recognise your partners and suppliers and that those with access should continue to have access. Our team can show you how to do this if you need our assistance.

Customer Control

- You will be required to approve our delegated access (GDAP/Azure Lighthouse), to allow our access
- As the customer you are in control and can remove Bytes' delegated access at any time through your admin centre. We would ask that you speak to us before you do this as it will limit our ability to support you.

How We Access Your Data

We access your data through services that operate under Microsoft's secure delegation model, giving customers full control over roles and permissions, and these are:

- GDAP via Partner Center: Used for Azure, D365 and Microsoft 365 management.
- Azure Lighthouse: Used for Azure subscription management only.
- Guest Access: Used for onboarding to the Azure Managed Service.

Native Access Limitations and controls

Bytes manage all Microsoft Cloud Agreements through Microsoft-provided tools: Partner Center (for Microsoft 365) and Azure Lighthouse (for Azure). These tools grant limited access to customer environments as defined in the Microsoft Cloud Agreement. Each of these tools' controls access and limits what we can do, and there are multiple points of control for you as the customer. These are summarised as follows:

Microsoft 365 (Microsoft Partner Center - GDAP)

- Partner Center users with any Agent role can view a list of customers' Entra (formally AAD) users.
- Admin Agent or Helpdesk Agent roles allow "Admin on Behalf Of" (AOBO) actions via Granular Delegated Admin Permissions (GDAP).
- GDAP provides similar access to a Global Admin, but does not allow direct viewing of:
    - User, Group, or Shared Mailboxes
    - SharePoint data
    - OneDrive for Business files
- Indirect Resellers may also be granted GDAP access.
- Bytes use Granular Delegated Admin Permissions (GDAP) via Partner Center for Azure, M365 & D365 support.
- Audit Logging is enabled by default for transparency.

Microsoft Azure (Azure Lighthouse)

- Azure Lighthouse enables delegated access to Azure subscriptions using a secure, role-based model.
- Bytes Agents appear as a single Foreign User Principal with the RBAC Owner role, inherited from the first user specified by the customer.
- Indirect Resellers may also have AOBO access via their own Foreign Principal.
- The RBAC Owner role allows download of most stored data types; Bytes strongly encourages customers to enable AES 256-bit encryption for all stored data.
- All actions within Azure subscriptions are tracked using native audit logging; customers should configure alerts for suspicious activity.
- Access is role-based and granted on a Just-in-Time basis.

GDAP Roles

The following GDAP roles are used to support customers requirements through these solutions:

SERVICE SUPPORT ADMINISTRATOR: Users with this role can create and manage support requests with Microsoft for Azure and Microsoft 365 services, and view the service dashboard and message center in the Azure portal and Microsoft 365 admin center. To find out more visit: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

ADMIN AGENT: This role grants users access to perform several key actions in the Account Settings, Billing, Customers, and Pricing workspace. To find out more visit: https://learn.microsoft.com/en-us/partner-center/accountsettings/permissions-overview#admin-agent-role

Customer Responsibilities

- Ensure that we have maintained access in place to ensure that we can support you.
- Approve GDAP and Azure Lighthouse requests when required.
- Follow the customer recommendations that we have suggested.
- Speak to us about any areas that you are unsure of, or to our compliance department or Group CISO if you need to know more about our security.

Security, Certifications and Compliance

The security model at Bytes is business aligned and based on the following principles:

- Risk and business impact assessed.
- Threat Intelligence prioritised.
- Technical telemetry focused.
- Security zoned based on asset criticality delivered.
- Attack surface management reduced / controlled.
- Compliance standards and industry accepted good practice implemented.
- Monitored, evaluated and responded to continuously.

Key Elements of our Cyber Security:

Some of the highlights of our data security include, but are not limited to:

GOVERNANCE, RISK AND ASSURANCE: Managed by the CISO and senior management team are engaged in the strategy at all levels of the business. Assurance activities feed back into the strategy to improve its approach, which is all reported and discussed at board level management forums.

THREAT AND RISK EVALUATION: Multiple systems monitor all aspects of our landscape and feed information into the teams in as close to real time as possible relating to current posture and any risk or threat exposures that need to be evaluated

DATA ENCRYPTION: All data is encrypted at rest and where possible all data is transport or payload encrypted in transit. This uses secure classical encryption in accordance with NIST SP800-131Ar2 and Bytes is in the process of moving to hybrid encryption that also encompasses Post Quantum Cryptography (PQC) standards like ML-KEM.

DEVICE SECURITY: These are centrally managed, secured and built to CIS Level 1 benchmark standards. They encompass EDR/XDR, network inspection and control, contextual awareness, firewall, DLP tools, web controls, behaviour analysis as well as full forensic capabilities.

APPLICATIONS AND SOFTWARE: These are centrally deployed and controlled according to technical security targets. No local control is possible and encompasses all software used, patching is conducted in line with risk management evaluation and EPSS ratings.

NETWORK SECURITY: Zoning and security context control with full network inspection and visibility at all layers of e network stack is implemented. Control points exist at multiple locations to enforce location, context and situational awareness controls.

SECURE REMOTE ACCESS: Separation zones are used to control access and provide control for remote access to customer environments. Dedicated IP addresses are available for customers.

SECURITY MONITORING: All layers of the stack from the application to the network connection are monitored, correlated and enriched with intelligence information. This includes user behavioural analytics and correlation of events from all telemetry systems that are then investigated and responded to on a continuous incident response basis.

IDENTITY AND ACCESS CONTROL: Identity and rights are highly controlled (through HR, vetting, IT and monitoring) and where possible FIDO2 compliant phishing resistant mechanisms of authentication are favoured. Users are only provisioned rights on a need to know and least privilege basis.

TRAINING: Multiple avenues of training are used including new starter, annual refresher, intelligence led, situational awareness training based on role, signposting as well as hints on good practice based on behaviours.

Certifications and Compliance

Bytes Software Services views both certifications and compliance with legislative, regulatory or elective compliance standards as essential to bolstering our cyber, infosec and resilience approaches, as well as a means of demonstrating what we do for our customers.

In relation to certifications Bytes holds:

CYBER ESSENTIALS: A demonstration of the foundational requirements of cyber security.

CYBER ESSENTIALS PLUS: A demonstration of externally audited foundational requirements of cyber security.

ISO 27001: A demonstration of our commitment to an information security management system that allows Bytes to show how confidentiality, integrity, and availability of data and information is managed.

IASME CYBER ASSURANCE LEVEL 2: An externally audited standard that reviews compliance with the GDPR / DPA 2018 as well as Cyber Security approaches to data and information security.

ISO 20000-1: Bytes certifies several of its service lines with ISO 20000-1 to demonstrate its service management capabilities which includes some of its security services delivered to customers.

Other areas of legislative, regulatory, elective compliance regimes or solution offerings (where our security is independently assessed) that we adhere to are:

NIS DIRECTIVE (UK): Bytes is categorised as a relevant digital service providers (RDSPs) and has chosen on a voluntary basis to comply with the requirements of the NCSC Cyber Assessment Framework (CAF), see https://www.ncsc.gov.uk/collection/cyber-assessment-framework for further information.

NIS2 (EU): We have assessed against the Information Security Forums (ISF) Standard of Good Practice (SoGP) to demonstrate compliance with the requirements of the NIS2 directive in the EU. We are waiting for formal certification to become available and then this will be achieved.

CHECK IT HEALTH CHECK (ITHC): Bytes choses to conduct the governments penetration testing requirements annually by having all aspects of its IT estate tested. While we do not have to do this, we see it as important that highly qualified, experienced and skilled testers verify what we do. More details can be found at: https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance/it-health-check-ithc-supporting-guidance

HELLIOS STAGE 3 FSQS AUDIT: We achieved stage 3 certification for external audit from one of the Big 4 audit companies that looks at all aspects of Bytes within the supply chain of its customers. This demonstrates to financial institutions our capabilities and security specifics and the level of security

that we have as part of their supply chain. Further information can be found here: https://hellios.com/pooled-audits-supplier

CREST Penetration Testing: Bytes are certified by CREST to conduct penetration testing, and the security of our solutions is audited annually. Our registration can be found here: https://www.crest-approved.org/member_companies/bytes-software-services-ltd/

PCI QSA Company: Bytes is certified by the PCI SSC to conduct security evaluation and audit an organisations payment card security. As part of this we must demonstrate our data security annually. Our registration can be found here: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors/

Center for Internet Security (CIS) Partner: Bytes is a member, partner and contributor to CIS, and can consult on benchmark usage and deployment.

ISF Member and Solution Provider: Bytes is not only a member but can also consult on the ISFs standards, risk management and resilience solutions. The ISF publishes the gold standard of information security and Bytes provides input to its threat research, tooling solutions and standards.

Bytes continue to seek relevant certifications and solution designations to demonstrate its credentials and forward looking approach to security. This list will continue to grow to demonstrate our continued commitment to cyber and information security both of Bytes and within our wider industry and communities.

Additional Resources

For further details and guidance on the topics covered in this policy, please refer to the links below:

Azure Lighthouse

1. What is Azure Lighthouse? - Azure Lighthouse | Microsoft Learn
2. Onboard a customer to Azure Lighthouse - Azure Lighthouse | Microsoft Learn
3. Azure Lighthouse - Microsoft Q&A

Partner Center: Granular Delegated Privileges (Service Support Administrator Role)

1. Granular delegated admin privileges (GDAP) introduction - Partner Center | Microsoft Learn
2. Obtain granular admin permissions to manage a customer's service - Partner Center | Microsoft Learn

Customer approval:

1. https://learn.microsoft.com/en-us/partner-center/customers/gdap-customer-approval#get-customer
2. https://learn.microsoft.com/en-us/partner-center/customers/gdap-customer-approval
3. Grant granular permissions to security groups - Partner Center | Microsoft Learn

Definitions and Glossary of Terms

Partner Center: streamlines several business processes to make it easier for Microsoft partners to manage their relationship with Microsoft and their customers.

AAD (now EntraID): Azure Active Directory is Microsoft's cloud-based identity and access management service, used to manage users, groups, devices, and access to applications and resources across Microsoft services and third-party platforms.

AOBO: Admin On Behalf Of is a Microsoft Azure and Microsoft 365 concept used primarily in Cloud Solution Provider (CSP) scenarios, where a partner organisation is granted administrative access to a customer's tenant or subscription to manage services on their behalf.

AES 256-bit encryption: 256-bit encryption is a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files

CSP: *Microsoft Cloud Solution Provider.*

FIDO2 compliant hardware keys: These are a compact hardware security device that provides multi-factor authentication (MFA) and passwordless login capabilities. It is used to enhance the security of online accounts and systems by requiring physical presence during the authentication process.

Foreign Principal: a security identity that represents a group of users from a CSP's tenant (not the customer's tenant). This identity is typically linked to a group called AdminAgents in the CSP's Azure Active Directory (AAD). It allows CSP users to access and manage Azure subscriptions that belong to their customers.

GDAP: a security feature that allows Microsoft partners (such as Cloud Solution Providers or Managed Service Providers) to access customer tenants with least-privileged, time-bound, and role-specific permissions. It follows Zero Trust principles, meaning access is granted only as needed and can be revoked or adjusted at any time

Information Rights Management (IRM): a Microsoft technology designed to protect sensitive digital content—such as documents and emails—by controlling how it can be accessed, used, and shared, even after it leaves your organization's network.

Just-in-Time basis: refers to a strategy or approach where resources, actions, or access are provided only when they are needed, and only for as long as necessary

MFA: Multi-Factor Authentication is a method of confirming a user's identity by combining something you know – e.g., a password or PIN; something you have – e.g., a smartphone, security token, or smart card; something you are – e.g., fingerprint, facial recognition, or other biometric data. To successfully authenticate, a user must present at least two of these factors.

Microsoft Azure Lighthouse: Azure Lighthouse allows service providers and organisations to manage Azure resources across multiple tenants using delegated resource management. This means service providers can perform tasks in customer environments without needing direct sign-in to each tenant, and without creating user accounts in those tenants.

RBAC: Role-Based Access Control. It's a method used in Microsoft Azure (and other systems) to manage who has access to what resources, based on their assigned roles

SaaS: Software as a Service is a cloud computing model where software applications are delivered over the internet, typically via a subscription. Instead of installing and maintaining software on individual devices or servers, users access it through a web browser

SIEM solution: Security Information and Event Management—is a cybersecurity system that provides organisations with centralised visibility, real-time threat detection, and incident response capabilities by collecting and analysing data from across their IT infrastructure.

TPM modules: Trusted Platform Module—is a specialised hardware component embedded in many modern computers, designed to enhance security by securely storing sensitive data such as encryption keys, passwords, and digital certificates.

UBA: User Behaviour Analytics (also called UEBA – User and Endpoint Behavioural Analytics) is a cybersecurity approach that involves monitoring and analysing user activities to detect abnormal behaviour that may indicate a security threat.