Document ID	POL091
Document Title	Cloud Solution Provider – Customer Data Access Control & Security Policy
Author	Nanda Narayanan
Version	5
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.
28/05/2026	2026054	Merged relevant POL078 content into REC042 to consolidate customer data access and security guidance.
29/06/2026	2026065	Included Bytes India (Proteam) Access

Distribution		
Date	**Version**	**Distribution**
10/12/2025	2025123	Compass – All Staff, Company Website
11/09/2026	2026065	Compass – All Staff, Company Website

Signed			
Date	**Version**	**Name**	**Role**
10/10/2025	2025123	Kathy Leach	Head of Support Services
10/09/2026	2026065	David Rawle	Chief Technology Officer

Contents

Introduction 3
Scope 3
Why we need access 3
Key Principles 4
Customer Recommendations 4
Customer Control 4
How We Access Your Data 4
Native Access Limitations and Controls 5
Microsoft 365 (Microsoft Partner Center- GDAP) 5
Microsoft Azure (Azure Lighthouse) 5
GDAP Roles 6
Additional Controls 6
Administrative Privileges 6
Remote Access 7
Arm's Length Systems 7
Approved Subcontractor for Microsoft 24/7 Support 7
Acceptance of Customer Data Access Control & Security Policy 8
Responsibilities 8
Customer Responsibilities 8
Bytes Responsibilities 8
Security, Certifications and Compliance 8
Key Elements of our Cyber Security: 9
Certifications and Compliance 10
Additional Resources 11
Azure Lighthouse 11
Partner Center: Granular Delegated Privileges (Service Support Administrator Role) 11
Customer Approval 11
Key Terms 11
Supporting Documentation 13

Introduction

Bytes Software Services (“Bytes") prioritises the security and privacy of customer data. Our information security policies and controls are designed to protect sensitive data and ensure compliance with recognised industry standards, including ISO 27001. To maintain the confidentiality, integrity, we have implemented robust security processes and controls that uphold high standards of protection.

This policy should be read in conjunction with Bytes’ Information Security and Data Access Policies. Employees found to be in breach of these policies may be subject to disciplinary action in accordance with the Bytes Staff Handbook.

This policy may be updated from time to time. Any changes affecting the extent of Bytes’ access will be detailed in the appropriate section.

Scope

The purpose of this document is to explain the extent to which Bytes Software Services may access customer data as part of its responsibilities as a Cloud Solution Provider, and to document the controls Bytes has put in place to prevent unauthorised access.

This policy applies to all parties that access customer data through rights provided via Microsoft Partner Center and Azure Lighthouse, including, but not limited to, all Bytes employees, contractors and partners. No Bytes employee is exempt from this policy.

Both systems are provided, supported and maintained by Microsoft. Our use of them may allow access to your data and information under specific circumstances. It is therefore important that we explain what those circumstances 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. Customers cannot raise these directly as a partner; in this case, Bytes must raise them on your behalf.
2. Provisioning licences into your tenant where these have been purchased, and managing licence counts and grants with Microsoft where required.
3. Providing support under the support contracts you hold with Bytes.
4. To investigate, troubleshoot and validate support issues across your Microsoft cloud services, including reviewing relevant configuration, service health, permissions and diagnostic information where required.
5. Onboarding to the Azure Managed Service, which requires guest access.
6. Making changes and performing deployments under the Azure Managed Service.

It is important that you understand the key principles we apply to this access, the steps we recommend you take, and the control you retain. 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.
- The customer signatory providing written authorisation must have the authority to do so.
- The written instruction must clearly authorise access to the data or Microsoft tool used to manage services.
- Accessing the Customer's data, or the MS tool used to manage services, is only carried out to the extent required to complete the specific task.
- All access is logged and monitored using Microsoft's native audit tools, and we can assist you with configuration to provide transparency over our activities.
- Bytes enforces strong security measures, including phishing-resistant MFA, encryption, endpoint protection, regular compliance training, and additional security controls.
- All access is performed using Bytes-managed devices and secure environments.
- Administrative roles are granted only when necessary.

Customer Recommendations

- We recommend that you implement AES 256-bit encryption for all stored data in Azure, Microsoft Customer Lockbox in Microsoft 365 where you have E5 licences, and BYOK (Bring Your Own Key) for data encryption in Dynamics 365. These measures help reduce the ability of Microsoft or partners to view data in your solution.
- We recommend that you include Bytes' access within your audit logs to ensure visibility of our activity. Our team can show you how to set this up within your tenants.
- We recommend that you configure alerts for Bytes' access so that you are notified when we access your systems and can confirm the reason for that access. Our team can show you how to set this up within your tenants.
- Conduct periodic reviews to ensure you recognise your partners and suppliers, and that those with access continue to require it. Our team can show you how to do this if you need assistance.

Customer Control

- Customers are required to approve our delegated access requests, including GDAP and Azure Lighthouse, before access can be enabled.
- As the customer, you remain in control and can remove Bytes' delegated access at any time through your admin centre. We ask that you speak to us before doing so, as removal may limit our ability to provide support.

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. These services 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 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 tool controls access and limits what Bytes 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' Microsoft Entra 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 uses Granular Delegated Admin Permissions (GDAP) via Partner Center for Azure, Microsoft 365 and Dynamics 365 support.
- Audit Logging is enabled by default for transparency.
- Customers may choose to remove Bytes GDAP. This will restrict the ability of Bytes Agents to assist Customers in any reactive support scenario.
- Customers may choose to remove any GDAP also granted to their Reseller. This may restrict the ability of the Reseller to complete their delivery of any services or their ability to complete any duly appointed tasks.

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.
- Customers may choose to remove Bytes' Foreign Principal from any of their subscriptions. This will restrict the ability of Bytes agents to assist customers in reactive support scenarios.
- Customers may choose to remove any Foreign Principal also granted to their Reseller. This may restrict the ability of the Reseller to complete their delivery of any services or their ability to complete any duly appointed tasks.

GDAP Roles

The following GDAP roles are used to support customer 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

Additional Controls

Administrative Privileges

1. Bytes operates a policy of least privilege for access to any administrative tool or function, including Partner Center and Azure Lighthouse. No member of staff will be granted an Agent role in Partner Center or Azure Lighthouse unless their tasks cannot be completed using any other functionality.
2. Access to Partner Center and Azure Lighthouse is restricted to Users in Bytes Azure Active Directory.
    a. It is Bytes HR Policy that each employee will have only one entry in the Company Active Directory.
    b. Bytes maintains a general IT Policy of a one-to-one relationship between Active Directory and Azure AD through directory synchronisation.
    c. Bytes users granted access to Partner Center and Azure Lighthouse will use a specifically provisioned account for the sole purpose of that access. This account is subject to higher-level security controls and is not used for day-to-day activity. Higher-level security includes:
        i. Minimum 14-character, complex passwords
        ii. Passwords changed every 45 days
        iii. Multi-factor authentication, which must include a physical security token
        iv. Access to the account is permitted only for the period of activity and disabled outside this timeframe
    d. The addition of Cloud Only Users in Bytes' Azure AD is reviewed and permitted by the Group Head of IT.
    e. Any Azure AD administrative privileges are reviewed and permitted by the Group Head of IT.
    f. As an extension of Azure AD administrative privileges any Partner Center roles will be permitted by the Bytes CSP Steering Group.
    g. Changes to any User's administrative permissions in Partner Center and Azure Lighthouse can only be completed by Bytes staff with suitable internal admin privileges.
    h. All Bytes employees with access to Partner Center and Azure Lighthouse will receive training in confidentiality, and this policy specifically, at appointment. Periodic refresher and update training will also be provided where appropriate.
    i. All Bytes employees with access to Partner Center and Azure Lighthouse will have their privileges reviewed every six months.

Remote Access

1. Due to the nature of Microsoft Partner Center and Azure Lighthouse, these services can be accessed from any network. However, the security of the network being used must be considered. Public Wi-Fi must not be used under any circumstances.

Arm's Length Systems

1. Most activities that can be completed on Partner Center have a corresponding API, allowing them to be completed using arm's length tools and systems.
2. Bytes has developed a publicly facing Cloud Dashboard (CDB), allowing customers to create quotes, change online services licence counts, and provision new subscriptions according to Microsoft price lists. Bytes employees also use this portal as part of internal processes to raise and complete customer orders where directed.
3. The Partner Center APIs have been integrated into CDB to allow employees to raise quotes, and process orders without any direct access to Partner Center. The APIs used for these tasks do not have any effect on Customer environments other than for generating pricing or provisioning services.
4. For any Partner Center tasks where Microsoft has not yet released an API, or where the API has not yet been integrated into CDB, only Bytes employees signed to this policy are permitted to complete the work.

Approved Subcontractor for Microsoft 24/7 Support

Bytes use Proteam Advisory Solutions LLP, also referred to as Bytes India, based in Hyderabad, India, as an approved subcontractor to support delivery of Microsoft 24/7 Cloud Technical Support. Proteam resources assigned to Bytes are dedicated exclusively to supporting Bytes services and are used to provide out-of-hours Microsoft Technical support for customers, ensuring continuity of service while maintaining alignment with Bytes operational, security and compliance standards.

Bytes retain ownership and control of the end-to-end resource lifecycle for Proteam resources supporting Bytes services. This includes interview and selection, recruitment and onboarding, and ongoing performance management and governance.

All Proteam personnel supporting Bytes services complete the Bytes standard staff onboarding training to ensure consistency in training, compliance and service delivery. This includes mandatory annual training covering information security, acceptable use, access control, data protection, information security awareness and ISO certification awareness. This ensures that personnel understand their responsibilities in protecting customer data and operating in line with Bytes' security standards.

From a technology and access perspective, devices used by Proteam resources to support Bytes services are procured, configured and managed in accordance with Bytes security requirements. Devices are managed within the Bytes secure network and are subject to Bytes security controls, monitoring and compliance policies.

Access to customer environments and data is governed in line with Bytes' data protection, access control and security policies, including applicable GDPR requirements. Access is controlled, auditable, role-based and limited to the purpose of delivering support services. Bytes remain responsible for ensuring that security and compliance standards are consistently applied.

Through this model, Bytes provides customers with assurance that all resources supporting Microsoft 24/7 Cloud Technical Support, regardless of location, operate under the same governance, security and data protection controls as Bytes' UK-based teams.

Bytes retains the right to audit Proteam's compliance with these controls, and Proteam is subject to [periodic/annual] review as part of Bytes' supplier assurance and ISO 27001 supplier management processes.

Acceptance of Customer Data Access Control & Security Policy

Acceptance and understanding of this policy are centrally recorded and enforced through internal training tools.

Responsibilities

The following responsibilities apply to both customers and Bytes in relation to the access covered by this policy.

Customer Responsibilities

- Ensure Bytes maintains the access required to support you effectively.
- Approve GDAP and Azure Lighthouse requests when required.
- Follow the customer recommendations set out in this policy.
- 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.

Bytes Responsibilities

- **Employees, Contractors and Partners** - must ensure that they adhere to this policy and seek clarification from their manager on any aspect that is unclear or requires further explanation.
- **Managers** - Managers are responsible for ensuring that those governed by this policy are aware of and comply with this policy.
- **CSP Steering Group** - has responsibility for ensuring the policy is fit for purpose.
- **Group Chief Technology Officer** - has board level responsibility for this policy. Group Chief Technology Officer (or Bytes Software Services equivalent) and CSP Steering Group are responsible for reviewing this policy as required or at least annually.

Security, Certifications and Compliance

The security model at Bytes is business-aligned and built upon the following principles:

- Risk and business impacts are assessed.
- Threat intelligence is prioritised.
- Technical telemetry is used to focus security activity.
- Security zoning is based on asset criticality.
- Attack surfaces are managed, reduced and controlled.
- Compliance standards and industry-accepted good practice are implemented.
- Security is 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, with the senior management team engaged in strategy at all levels of the business. Assurance activities provide feedback into the strategy to continuously improve Bytes' approach and are reported and discussed at board-level management forums.

Threat and Risk Evaluation: Multiple systems monitor our landscape and feed information into teams in near real time, relating to current posture and any risk or threat exposures that require evaluation.

Data Encryption: All data is encrypted at rest and, where possible, transport or payload encrypted in transit. This uses secure classical encryption in accordance with NIST SP 800-131A Rev. 2. Bytes is also progressing towards hybrid encryption that encompasses post-quantum cryptography standards such as ML-KEM.

Device Security: Devices are centrally managed, secured and built to CIS Level 1 benchmark standards. They include EDR/XDR, network inspection and control, contextual awareness, firewall, DLP tools, web controls, behaviour analysis and forensic capabilities.

Applications and Software: Applications and software are centrally deployed and controlled according to technical security targets. Local control is not permitted, and patching is conducted in line with risk management evaluation and EPSS ratings.

Network Security: Zoning and security context controls are implemented, with full network inspection and visibility across all layers of the network stack. 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 access rights are highly controlled through HR, vetting, IT and monitoring processes. Where possible, FIDO2-compliant, phishing-resistant authentication mechanisms are favoured. Users are provisioned access on a need-to-know and least-privilege basis.

Training: Multiple training routes are used, including new-starter training, annual refreshers, intelligence-led training, role-based situational awareness, signposting and good-practice prompts based on behaviours.

Certifications and Compliance

Bytes Software Services views certifications and compliance with legislative, regulatory and elective standards as essential to strengthening our cyber security, information security and resilience approaches, and to demonstrating our commitments to 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 provider (RDSP) and has chosen voluntarily to comply with the requirements of the NCSC Cyber Assessment Framework (CAF). Further information is available from the NCSC Cyber Assessment Framework.

NIS2 (EU): Bytes has assessed against the Information Security Forum's Standard of Good Practice (SoGP) to demonstrate alignment with the requirements of the NIS2 Directive in the EU. Bytes is awaiting formal certification becoming available and intends to achieve it when possible.

CHECK IT HEALTH CHECK (ITHC): Bytes chooses to conduct the government's penetration testing requirements annually by having all aspects of its IT estate tested. Although this is not mandatory for Bytes, we consider it important that highly qualified, experienced and skilled testers verify our approach.

HELLIOS STAGE 3 FSQS AUDIT: Bytes achieved Stage 3 certification through an external audit by one of the Big 4 audit companies. The audit considers all aspects of Bytes within its customers' supply chains and demonstrates to financial institutions our capabilities, security specifics and supply chain security posture.

CREST PENETRATION TESTING: Bytes is certified by CREST to conduct penetration testing, and the security of our solutions is audited annually.

PCI QSA COMPANY: Bytes is certified by the PCI SSC to conduct security evaluations and audit organisations' payment card security. As part of this, Bytes must demonstrate its data security annually.

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 an ISF member and can also consult on ISF standards, risk management and resilience solutions. The ISF publishes leading information security standards, and Bytes provides input to its threat research, tooling solutions and standards.

Bytes continues to seek relevant certifications and solution designations to demonstrate its credentials and forward-looking approach to security. This list will continue to grow as part of our ongoing commitment to cyber and information security within Bytes and across 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

Key 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 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. A method used in Microsoft Azure and other systems to manage who has access to resources based on 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.

Supporting Documentation

- POL010 - Information Security Policy
- POL018 - Access Policy
- Data Breach Procedure
- Data Subject Access Request Procedure
- Data Retention Policy