CyberOne

Identity as a Service

Microsoft Entra ID

G-Cloud 15

Service Description

Service Description
Identity as a Service | Assure 365

This Schedule forms part of Schedule 3 to the Agreement between Customer and Provider and sets out a description of the Services, Service Levels and Service Credits in relation to the Identity as a Service module from Assure 365 as given on a Service Order.

1. Additional Definitions

The following definitions apply in this Schedule:

Assure 365: Assure 365, or A365, is a collection of modular managed services designed to enable Customers to outsource their cybersecurity and IT operations. Each module taken be taken as a standalone service or packaged within in a bundle of services. Some examples of modules include SOC as a Service, Endpoint as a Service, Data Security as a Service.

Identity and Access Management: Identity and Access Management or IAM is a platform that controls access to organisational resources such as applications and data. This access is granted through user identities which must be authenticated and authorised to access the resources they request.

RBAC: Role-Based Access Control or RBAC is a method of predetermining the level of access an end user may have over a given resource by configuration permissions to allow or block access.

BAU: Business as usual is the normal operation of typical and routine tasks or functions within an organisation, for example in relation to the smooth daily operation of an Identity and Access Management (IAM) platform.

2. Additional Commercial Terms Relating to Endpoint as a Service

N/A

3. Additional Commercial Obligations Relating to Endpoint as a Service

3.1 The Customer will retain an active Entra ID tenant for the duration of the Service.

3.2 The Customer will retain valid Entra ID licenses such as M365 Business Premium, Entra ID P1, or Entra ID P2. The scope of this service is tied to the feature set available with the Customers' Microsoft licenses.

3.3 The Customer will be responsible for any costs relating to the acquisition and ongoing subscription of M365, or other, Microsoft licenses required to enable the Provider to provide the Service.

3.4 The Customer will provide the Provider with the appropriate level of access to enable the provision of the full breadth and depth of the service, including onboarding and ongoing management, the expected level of access required is the 'Global Administrator' Entra ID role.

4. Identity as a Service

4.1 The Identity as a Service module from Assure 365 leverages the Microsoft Entra ID identity and access management platform to provide a fully outsourced identity-led security and operations managed service to configure and maintain the Customers Entra ID environment in a secure manner.

4.2 Onboarding - Identity as a Service:
4.2.1 The Provider will issue a project plan outlining the high-level technical steps necessary to complete the onboarding of the service

4.2.2 The Customer will review and agree to the issued project plan.

4.2.3 The Customer will grant appropriate access to the Provider.

4.2.4 The Provider will deliver a standardised onboarding in which security policies and configuration of Entra ID will be assessed, and if appropriate, hardened to align with best practice configuration.

4.3 Ongoing - Identity as a Service:
4.3.1 Maintenance of security policies and configuration, and continued alignment to established best practice. Any requests by the Customer to deviate from a recommended best practice will require business justification from the Customer and may be challenged by the Provider.

4.3.2 24 x 7 x 365 operation of joiners-movers-leavers (JML), inclusive of external parties such as contractors and vendors.

4.3.3 24 x 7 x 365 monitoring of user behaviour through Entra ID audit logs, and blocking of suspicious or malicious user accounts.

4.3.4 24 x 7 x 365 operation of BAU identity tasks such as password resets, investigation and unblocking of disabled accounts.

4.3.5 Management of administrative permissions through Entra ID Privileged Roles.

4.3.6 Management of non-administrative permissions through Entra ID RBAC.

4.3.7 Quarterly review of security policy configuration to ensure settings are fit for purpose.

4.3.8 Advice provided to Customer to harden their systems to prevent security Incidents where potential vulnerabilities or lack of best practice by Customer have been identified by the Provider during operation of Entra ID.

4.3.9 Where applicable, the Provider will implement appropriate Security Policies, within agreed technology stacks, where the Provider deems it beneficial to the ongoing success of the Identity as a Service module.

4.3.10 Business Hours support for general Customer enquiries relevant to Entra ID.

4.3.11 Environment maintenance, including configuration tuning, cleanup of unnecessary identities or similar objects.

4.4 Unless otherwise expressly agreed, the following are not included in Identity as a Service:
4.4.1 Configuration and management of endpoint XDR or anti-virus platform or similar.
4.4.2 Configuration and management of non-Entra ID identity and access management platforms.
4.4.3 Incident response actions for identity-based attacks or threats.
4.4.4 Remedial/recovery work following a Security Incident.

5. Exclusions

5.1 Only the activities, deliverables, and responsibilities expressly detailed within this Service Description are included. Any service elements not specifically stated are excluded from the scope unless agreed in writing by both parties.

6. Service Levels

The Provider will respond according to the following Service Levels on Ticket Open and the priority levels assigned by the Provider.

Response Time (contractual)

	Priority Level	Target SLA	Expected Performance
Enhanced Hours 24x7x365	P1 – High	15 Mins	95%
	P2 – Medium	30 Mins	95%
Standard Business Hours	P3 – Moderate	1 Hour	95%
	P4 – Minor	2 Hours	95%

Triage Time (non-contractual)

	Priority Level	Target SLA	Expected Performance
Enhanced Hours 24x7x365	P1 – High	1 Hour	90%
	P2 – Medium	2 Hours	90%
Standard Business Hours	P3 – Moderate	8 Hours	90%
	P4 – Minor	24 Hours	90%

Monthly Response Time performance is calculated as follows:

For each Priority Level the performance for Response Time ("Actual Performance") is calculated as:

Actual Performance = Number of incidents recorded for each Priority Level within SLA Target in any month / number of Incidents recorded for the Priority Level in total in any month * 100

This is then compared to the Expected Performance for each Priority Level given in the Response Time table above.

7. Service Credits

If the Actual Performance is less than the Expected Performance in any month for either of the P1 or P2 Priority Levels, Service Credits equivalent to (1) week's Charges for the Service shall be due to Customer, such that maximum Service Credits of two weeks Charges for the Service may be payable in any month.

Service Credits cannot be obtained in relation to:

- Triage Time;
- In connection with P3 or P4 Priority Levels; and,
- During the first 3 months of the Service being live.

Identity as a Service

Cyber Resilience Starts with Identity Management. Securing Access. Reducing Risk. Enhancing Compliance.

Powered by Microsoft Entra ID. Realised by CyberOne.

CyberOne's Managed Identity & Access Service provides robust protection for user access, aligned with Zero Trust principles to safeguard sensitive data through strong controls. Powered by Microsoft Entra ID, this managed service delivers a scalable approach to identity security, ensuring resilient protection with minimal internal overhead.

Part of CyberOne's Assure 365 suite, our fully outsourced Managed Microsoft Security solution offers modular cyber security services tailored to your needs. It delivers comprehensive, scalable protection to strengthen resilience and empower you to focus on your core business objectives.

What is Microsoft Entra ID?

Microsoft Entra ID (formerly Azure Active Directory) is Microsoft's industry-leading Identity & Access Management (IAM) platform.

Trusted by organisations of all sizes, Entra ID secures access, enhances productivity and supports compliance by managing user identities and enforcing access policies across applications and devices.

CyberOne's Identity as a Service offering forms a crucial module within our Assure 365 solution, enabling organisations to gain a powerful, robust and expertly managed identity and access service, building a resilient foundation that is adaptable to evolving business needs.

advanced

Key Features of CyberOne's Identity as a Service

CyberOne's Managed Identity & Access Service provides a comprehensive set of capabilities to safeguard user identities, streamline access and enforce security controls to minimise your organisations attack surface.

Security Assessment & Configuration
Identification of current state risks, remediation and your desired future state.

Identity Governance & Administration
Lifecycle management for resource access inc. workflow setup for internal and external users.

Privileged Identity Management
Setup and ongoing auditing of access and alerts for privileged and administrative users.

Management of External Access
Secure integration with partners through Entra ID, facilitating secure B2B collaboration.

Multi-Factor Authentication
Management of MFA policies for all user types, inc. external parties.

Joiners, Movers & Leavers (JML)
Full management of users inc. group management and permissions

Managed SSO & App Onboarding
Integration of applications into Entra ID SSO and ongoing management of the app lifecycle.

Role-Based Access Control
Assignment and management of custom permissions for standard users and groups.

Conditional Access
Management, tuning and ongoing review of conditional access to enforce Zero Trust.

User Behaviour & Identity Analytics
Continuous monitoring of risky behavior e.g. suspicious logins or compromised credentials.

Unlock Business Value with CyberOne

Enhanced Security
Minimises unauthorised access with 24x7 monitoring and proactive threat detection and robust access control.

Scalable Compliance
Maintains consistent identity governance with automated workflows, supporting both internal and external users.

Tighter Control & Access
Enforces strict controls for high-risk users, reducing unauthorised access to sensitive areas.

Secure Collaboration
Provides controlled access for external partners, ensuring security and compliance in all B2B interactions.

Actionable Insights
Delivers valuable analytics to support informed security and compliance decisions.

Operational Efficiency
Automates user provisioning and de-provisioning, reducing workload with streamlined processes.

Improved User Experience
Simplified, secure access with SSO and role-based permissions, making it easy to access required resources.

Reduced Risk
Aligns permissions with user roles to reduce access risks and ensure appropriate access levels.

Business Continuity
Ensures reliable, uninterrupted access, supporting rapid recovery and resilience against disruptions.

Cost Savings
Reduces in-house expertise and lowers expenses associated with breaches and regulatory fines.

Why Choose CyberOne's Identity as a Service?

Choosing CyberOne's Managed Identity & Access Service provides your organisation with the expertise, resilience and streamlined operations needed to secure access, reduce risk and drive compliance with ease.

1. Expertise You Can Trust
CyberOne's certified Microsoft specialists optimise Entra ID for robust identity security, proactively addressing evolving threats and best practices.

2. Guaranteed Security Outcomes
As an NCSC Assured Service Provider, CyberOne enforces stringent security and compliance standards to protect sensitive data across your organisation.

3. Proactive Cyber Resilience
With support from our CREST-accredited SOC, CyberOne provides 24x7 monitoring and rapid response, enabling your organisation to adapt to emerging threats and maintain resilient identity security.

4. Efficient Onboarding and Offboarding
CyberOne streamlines user access management for new joiners and access removal for leavers, which enhances productivity and reduces IT overhead.

5. Maximised Microsoft ROI
Fully leverage your Microsoft investment with CyberOne's certified expertise across Entra ID, Microsoft 365 and the wider Security suite.

6. Ongoing Monitoring & Reporting
Comprehensive reporting keeps your organisation informed and compliant, providing full visibility and insight into access events and supporting regulatory requirements.

About CyberOne

CyberOne is a Microsoft Security Solution Partner and member of the Microsoft Intelligent Security Association (MISA). We deliver one of the UK's most advanced AI-augmented Managed eXtended Detection & Response (MXDR) services, recognised with Microsoft-verified Managed XDR solution status, enabling organisations to move with confidence from risk to resilience. Powered by Microsoft's market-leading security technologies and realised by CyberOne's accredited experts, we help businesses anticipate and contain modern threats so they can thrive.

With 24x7x365 Global SOC coverage, NCSC accredited Cyber Incident Response, CREST SOC and Penetration Testing accreditations and guaranteed SLAs, CyberOne combines Microsoft Security with expert consulting, professional and managed services to protect operations, achieve compliance and build lasting resilience.

Accreditations & Certifications

CyberOne's services are backed by the world's leading standards bodies including NCSC, CREST and ISO as well as our key technology partners, whilst our experts are backed by industry-leading certifications, cementing our role as leaders in cyber security.

CyberOne

hello@cyberone.security

+44 (0) 3452 757575

cyberone.security