Cloud Computing Policy

Policy that governs use of Cloud computing within Microlink

# Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change |
| 0.1 | 09/11/2022 | DH | Initial Draft |
| 1.0 | 17/06/2023 | DH | First revision |
|  |  |  |  |
|  |  |  |  |

# Introduction/Overview

The purpose of this policy is to ensure that Microlink data is not inappropriately shared or stored using public cloud computing and/or file sharing services.

The purpose of this policy is to ensure Microlink, and its employees meet our regulatory requirements, adhere to cloud security best practice for accessing and processing data stored on the cloud. It will layout responsibilities and actions needed to ensure the data access and processed on cloud can maintain confidentiality, Integrity, and availability.

Contents

[Version Control 1](#_Toc124431270)

[Introduction/Overview 1](#_Toc124431271)

[1. Definitions 1](#_Toc124431272)

[2. Applicability/Scop 2](#_Toc124431273)

[3. Controls 2](#_Toc124431274)

[3.1. Acceptable Cloud Use 2](#_Toc124431275)

[3.2. Technical controls 3](#_Toc124431276)

[4. Exceptions 3](#_Toc124431277)

[5. Failure to comply. 3](#_Toc124431278)

[6. Monitoring 3](#_Toc124431279)

[7. List of Approved Vendors and services 3](#_Toc124431280)

[8. Procurement 4](#_Toc124431281)

[8. Related Policies 4](#_Toc124431282)

# Definitions

|  |  |
| --- | --- |
| *Definition* | *Meaning* |
| *Cloud computing* | ***Cloud computing*** *is a computing model which enables user easy on demand access to computing recourses such as networks servers storage applications and services that can be quickly provisioned and decommissioned with little computing knowledge and interaction.*  *Cloud computing can be defined as the use of information technology hosting or servers of any type that is not controlled by Microlink (physically owned and maintained by Microlink)* |
| *IaaS* | ***Infrastructure as a service*** *is one of 3 fundamental cloud service models. It is a means of delivering infrastructure as an on-demand service. Specifically server, network and storage resources. It can be an entire piece of hardware dedicated to the user/tenant or can be a securely shared resource for multiple users/tenants. Examples: AWS EC2.*  *Rackspace, Google Compute Engine (GCE), Digital Ocean, Microsoft Azure, Magento 1 Enterprise Edition\*, UK2* |
| *PaaS* | ***Platform As A Service*** *is one of the 3 fundamental cloud service models. It is cloud delivery model for applications made of services managed by a 3rd party. It allows developers to use pre-made blocks to decrease development time. Examples: AWS Elastic Beanstalk, Heroku, Windows Azure (mainly used as PaaS), Force.com, Google App Engine, OpenShift, Apache Stratos, Adobe Magento Commerce Cloud.* |
| *SaaS* | ***Software as a service*** *is one of the 3 fundamental cloud service models. It allows users to run software available over the internet. Examples: BigCommerce.*  *Google Workspace, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot* |
| *Single Sign on* | *SSO provides the business a safe way to use a single set of credentials (username and password) to authenticate across multiple systems without each system actually knowing credentials.* |

# Applicability/Scop

This policy covers any system that handles Microlink data. All systems and services within a cloud environment are subject to the requirements specified in this policy. The policy applies to new and existing cloud services.

Every user who interacts with company IT systems or services is also subject to this policy and the security controls defined. controls are product agnostic and are applicable for all approved cloud systems.

# Controls

Controls are applicable to approved cloud services

## Acceptable Cloud Use

* + 1. Microlink staff, Subcontractors or partners are not permitted to enter any cloud platform service contracts for storing, processing, or sharing of microlink or microlink client data.
    2. Department that wishes to use a cloud platform service must use the appropriate and approved vendors that have been vetted and contracted by Internal IT department and Internal legal team. See Section 7 List of Approved Vendors/Services.
    3. All cloud computing resources, and service must be contracted through centralised IT Department
    4. The use of cloud computing service must comply with existing information security policies including but not limited to:
       1. Information Classification & Handling Policy
       2. Document Retention and Records Management Policy
    5. The use of cloud computing service must comply with all laws and regulations governing Microlink.
    6. Non-Microlink, personal clouded service accounts may not be used for storage, processing or sharing microlink related or Microlink owned data.

## Technical controls

The following is a list of technical controls that should be implemented in all approved cloud services where available. Different “as a service” offerings will require different controls; all available controls should apply.

* + 1. Audit logs for Sign-in should be enabled where possible.
    2. Access control methods to be used shall include
       1. Multifactor Authentication
       2. Conditional Access
       3. Role based permissions
       4. SSO (Same or Single) sign on
    3. Modern Encryption standards must be in place for
       1. Data in transit. Such as TLS1.2
       2. Data at rest. Such as AES-256 Encryption.
    4. Tools that offer the configuration monitoring and assessment, traffic analysis and alerts for configuration issues should be used.

A vendor that is required to store or process sensitive data should use select best practices from the 14 security principles listed by the National Cyber Security Centre (NCSC).

## Risk assessment

Risk assessment must be conduct by each department head who wishes to utilise each cloud platform and risks must be recorded in the required risk register.

# Exceptions

* 1. Any exceptions regarding adoption of new cloud platform/service must be approved by exec team and CISO.

# Failure to comply.

Failure to comply with any of the above will result in action being taken under MLPC’s Disciplinary procedure, which could include dismissal.

# Monitoring

Due to the security concerns with the use of cloud computing a security review must be conduct either directly with the vendor or using official published documentation, prior to implementation.

# List of Approved Vendors and services

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Platform Type** | **Vendor** | **Service name/Description** | **Primary uses** | **Allowed applicability** |
| * SaaS | * Microsoft | * Microsoft 365 including following software platforms * SharePoint * Forms * Teams * Outlook 365 * OneDrive * Only when accessing via Microlink Account and MFA enabled. | * Internal and restricted External collaboration on files and documents. * Internal and external Meetings and communications. * Internal and external sharing of documents. | * **Permitted** * Unrestricted Grade 0, * Restricted Grade 1, * Confidential Grade 2 – Commercial, * Highly Confidential Grade 3 – Commercial. * **Prohibited** * Unclassified information, * Highly Confidential Grade 3 – SPII, * Highly Confidential Grade 3 – PCI, * Confidential Grade 2 – PII, |
| * IaaS | * Microsoft | * Azure | * Offsite Storage, Networking, and compute | * Select and restricted data |
| * SaaS | * Access UK Ltd | * PeopleHR | * Microlink employee HR system | * All types, Excluding customer data. |

# Procurement

Microlink will look to endorse venders who deliver services that can meet the following standards. These should be listed, or equivalent terms, in terms of service or contract where applicable.

* 1. Any contractual agreement for cloud services should specify that the datastore must be in onshore locations that are within the boundaries of the United Kingdom.
  2. Microlink must remain the data controller of any data that is stored or processed by the cloud service provider. The cloud service provider must remain data processor.
  3. The service must ensure that data is encrypted at rest and in transit.
  4. The supplier cannot use Microlink data in any way that violates any laws or Microlink policies including but not limited to:
     1. Acceptable use policy
     2. Application security policy
     3. Password and credential policy
     4. Document Retention and Records Management Policy
     5. Other IT related polices
  5. Plans must be created to the integration of the service into business continuity and disaster recovery plans.
  6. Microlink must determine how data would be recovered from the vendor and/or transferred to a different vendor.
  7. Acknowledgement that the service provider must only use provided data for the explicit purpose defined in the terms or contract.

# Related Policies and references.

* Information Classification & Handling Policy
* Acceptable use policy
* https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles