Third Party Information Security Management Policy

# Version Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change | Approved by: |
| 1.3 | June 2023 | Abigail Hoff | Review and Update | Michael Moore, Legal Counsel |
| 1.4 | June 2024 | Abigail Hoff | Review and Update | Michael Moore, Legal Counsel |

Contents

-----

[Version Control 1](#_Toc137106490)

[Introduction & Executive Summary 1](#_Toc137106491)

[1. Information Security Rik Assessments for Third Parties 1](#_Toc137106492)

[2. Roles and Responsibilities 2](#_Toc137106493)

[3. Review 2](#_Toc137106494)

# Introduction & Executive Summary

The purpose of this policy is to define the principles for protecting Microlink’s assets where they are accessible by suppliers. This policy is applicable to all Microlink suppliers; information security requirements shall be agreed as appropriate for each supplier. These requirements shall be documented where required, for example:

1. Microlink Terms and Conditions.
2. Contracts with the Third Party.
3. Confidentiality Agreements.
4. Non-Disclosure Agreements.
5. Exchange Agreements.
6. Service Definitions, or
7. Service Level Agreements.

# Information Security Risk Assessments for Third Parties

We shall confirm third parties are adhering to the information security requirements set up on them through our annual supplier audit and corresponding risk assessment. Answers will be given a score of Green, Amber or Red. A score of green would mean that the answer is fully acceptable and needs no follow up; Amber means the answer is acceptable but needs follow up in the audit the following year; A score of red means this is a critical item and must be monitored throughout the year. The item must be rectified before the following years audit and the progress will be monitored throughout the year. Failure to rectify the item, or make significant progress towards rectification, would result in the potential termination of business with the supplier. This risk assessment shall be used to identify security risks related to supplier access to Microlink information. The information security risk assessment shall be used to:

1.1 Identify suppliers or groups of suppliers with access to Microlink Information.

1.2. Identify the risks associated with the access granted.

1.3 Identify the controls implemented to mitigate the risks.

1.4 Score the residual risk.

1.5 Identify the risk owner.

1.2 The risk assessment methodology documents the authorities for making decision in response to risk assessments (treat/accept/transfer/etc.) Risk owners shall have the authority to make decisions on risk treatment/acceptance. The decisions are recorded in the Microlink Information Security Risk Register, and this is visible to the main security governance forum, the BMS review.

# Roles and Responsibilities

2.1 It will be the role of the Legal and Compliance team to ensure that the Information Security requirements of the suppliers are communicated to the suppliers in a clear manner. It will also be the role and responsibility of the Compliance department to ensure that all suppliers continue to comply with the Information Security requirements.

2.2 It is the responsibility of the Directors, and the Compliance department, to maintain the risk assessment in accordance with the rules in the Risk Assessment Methodology.

# Review

3.1 This policy will be reviewed, and updated where necessary, on at least an annual basis.

|  |  |
| --- | --- |
| Name: | Michael Moore |
| Position: | Legal Counsel |
| Date: | 17/06/2024 |
| Signature: |  |