Third Party Management Policy

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change | File Location | Approved by/ Date |
| V0.1 | 07/11/2012 | Stav Papageorgaki | Initial Draft | \\so-srv-files\ISO Standards\ISM\Policy Documentation\Current Policies |  |
| V1.1 | 13/11/2012 | Stav Papageorgaki/David Bartlett | Overall amendments |  | CISO-21/11/2012 |
| 1.1 | 10-05-2014 | ISM | Reviewed: No changes |  |  |
| 1.1 | 15-05-2015 | ISM | Reviewed: No change |  |  |
| 1.2 | 16/06/2021 | Stav Papageorgaki | Policy Updated – New roles assigned | Sharepoint |  |
| 1.3 | 15/11/2024 | Abigail Hoff | Review and Update |  | Michael Moore, Legal Counsel |

 **Document Owner Legal and Compliance Team**

Contents

[1. Introduction 3](#_Toc182556525)

[2. Objective 3](#_Toc182556526)

[3. Applicability 3](#_Toc182556527)

[4. Definition of a Third Party 4](#_Toc182556528)

[5. Responsibilities 4](#_Toc182556529)

[5.1 Compliance Manager 4](#_Toc182556530)

[5.2 Legal Services 4](#_Toc182556531)

[5.3 System Owners – Internal IT 4](#_Toc182556532)

[6. External Parties 5](#_Toc182556533)

[6.1 Identification of risks related to external parties 5](#_Toc182556534)

[6.2 Addressing Security When Dealing with Customers 5](#_Toc182556535)

[7. Addressing security in third party agreements 6](#_Toc182556536)

[8. Third Party Service Delivery Management 7](#_Toc182556537)

[9. Monitoring Third Party Services 7](#_Toc182556538)

[10. Security Policy Requirements 8](#_Toc182556539)

[11. Staff Screening 8](#_Toc182556540)

[12. Access to Microlink Information and Information Systems 8](#_Toc182556541)

[13. Electronic Access 9](#_Toc182556542)

[14. Network Access Control 9](#_Toc182556543)

[15. Anti-Virus Management 9](#_Toc182556544)

[16. Security Incident Management 10](#_Toc182556545)

[17. Information Confidentiality 10](#_Toc182556546)

[18. Media and Paper Document Handling 11](#_Toc182556547)

[18.1 Disposal of Microlink Media 11](#_Toc182556548)

[18.2 Removal of Property 11](#_Toc182556549)

[19. Clear Desk and Clear Screen 11](#_Toc182556550)

[20. Use of Microlink Email and Internet Services 12](#_Toc182556551)

[21. Change Control 12](#_Toc182556552)

[22. Audit & Monitoring 12](#_Toc182556553)

[23. Compliance 12](#_Toc182556554)

[23.1 Policy Compliance 12](#_Toc182556555)

[23.2 Exceptions 13](#_Toc182556556)

[23.3 Penalties 13](#_Toc182556557)

[24. Review 14](#_Toc182556558)

[25. Signature 14](#_Toc182556559)

# Introduction

Any loss, compromise or misuse of Microlink’s information or information systems and assets, however caused, could have potentially devastating consequences and may result in financial loss and legal action. Access to Microlink’s systems, facilities and information by third parties potentially poses a security threat and as such, needs to be controlled.

# Objective

This policy aims to ensure that access to Microlink’s facilities, systems and information assets by Third Parties is appropriately controlled so that confidentiality, integrity, availability and accountability of information remain intact.

Factors relating to the following corporate responsibilities must be identified, understood via a Risk Assessment (RA) and approved through Risk Management.

* legal and regulatory requirements
* contractual obligations
* security policy requirements
* information governance requirements
* network operations

This policy covers the following aspects of third Party relationships:

* third party risk assessments
* contract
* network service provision
* authorisation of connections
* security of access by non-permanent employees (Physical and electronic).

#  Applicability

This document is applicable to all of Microlink’s activities and personnel at Microlink House and includes all assets and infrastructure.

Compliance with this policy is required of all Microlink employees, including temporary staff, all sub-contractors, contractors responsible for the negotiation, initiation, authorisation, implementation and maintenance of Third-Party relationships and services pertained.

#  Definition of a Third Party

A ‘Third Party’ is an organisation or individual (non–permanent employee) external to Microlink. This will include:

* customers
* business partners
* onsite contractors
* staff agencies
* IT & building facilities suppliers.
* regulatory body representatives and Non-Governmental Organisations’ representatives

# Responsibilities

## 5.1 Compliance Manager

Provides the initial Risk Assessment and approval for Third Party organisations for contractual negotiations to proceed.

Ensures continual annual and ad hoc risk assessments are conducted to maintain accurate records.

Ensures before access is approved and granted all necessary security requirements defined in this policy are met in the contractual agreement.

Collaborates with associated teams regarding contractual and security requirements.

Ensures business need is defined before approval of access.

Acts as the escalation point for reporting security incidents and contractual breaches with appropriate investigation and review.

Maintain and re-negotiate contracts upon changes to Microlink’s infrastructure or requirements.

Manages and liaise with all relevant parties to bring the Third Party agreement to completion.

## 5.2 Legal Services

Construct and negotiate a contractual agreement that will ensure no misunderstanding between Microlink and the Third-Party Supplier Organisation.

Ensure all security conditions outlined in this policy are contained within the contract.

Collaborate with all parties involved to ensure completeness and accuracy of the contract before approval and implementation.

Ensure that terms and conditions defined in the contract comply with Microlink’s processes and all legal and regulatory responsibilities.

## 5.3 System Owners – Internal IT

The System Owners have a responsibility to:

Ensure services required and supplied to Microlink follow current contractual agreements.

Ensure that any selected third parties have the capability to comply with Microlink security requirement as described in the Information security set of policies.

Provide access to Microlink data for the Third parties, in line with the company’s security policies and the contractual obligations, and as per Clause 3 of this policy.

Responsibilities for any of the above functions can be delegated to suitable authorised individuals, as appropriately chosen by the owners, and as per specific case requirements.

# External Parties

## 6.1 Identification of risks related to external parties

The risks to the organisation’s information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

Where there is a requirement for a Third Party to access Microlink’s facilities, information or information systems a Security Risk Assessment (RA) shall be conducted by the Head of IT to identify any additional security requirements or additional controls needed. The RA shall be performed before the granting of additional services/connectivity and should take into account the following issues:

* The information processing facilities the Third Party is required to access.
* The type of access required, to information and information processing facilities e.g.:
* physical access (computer rooms, cabinets, offices etc)
* electronic access (database access, general information)
* Network connectivity between Microlink and Third Party (e.g. Permanent connection, remote access).
* Classification, value and sensitivity of the information to Microlink and its operations.
* What controls are deployed by the Third Party for storing, processing, communicating and sharing information belonging to Microlink.
* Security measures employed by the Third Party.
* Contractual obligations and legal/regulatory compliance requirements.
* Security management controls, including compliance with ISO 27001 Microlink’s security policies and confidentiality agreements.
* Practices and procedures to deal with information security incidents.
* Ownership of systems and information must be clearly defined.

## 6.2 Addressing Security When Dealing with Customers

All identified security requirements should be addressed before giving customers access to the organisation’s information or assets.

The following matters should be considered when addressing security before giving customers access to any of Microlink’s information and information assets:

* Asset protection, including:
* procedures to protect the organisation’s assets, including information and systems
* management of known vulnerabilities
* Procedures to determine whether any compromise of the assets, e.g. loss or modification of data, has occurred
* integrity
* Restrictions on copying and disclosing information.
* Description of the product or service to be provided.
* The different reasons, requirements, and benefits for customer access.
* Access control policy, covering:
* permitted access methods, and the control and use of unique identifiers such as user Ids and passwords
* an authorisation process for user access and privileges
* a statement that all access that is not explicitly authorised is forbidden
* a process for revoking access rights or interrupting the connection between systems.
* Arrangements for reporting, notification, and investigation of information inaccuracies (e.g. of personal details), information security incidents and security breaches.
* A description of each service to be made available.
* The target level of service and unacceptable levels of service.
* The right to monitor, and revoke, any activity related to the organisation’s assets.
* Responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. Data protection legislation.
* Intellectual property rights (IPR) and copyright assignment and protection of any collaborative work.

# Addressing security in third party agreements

Agreements with third parties involving accessing, processing, communicating or managing the organisation’s information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

Arrangements involving third party access to Microlink’s information or information systems are based on a formal Contract containing (or referring to) all of the appropriate security requirements to ensure Information Security compliance.

The following terms must be considered for inclusion in the agreement:

* Microlink’s security policies (or a document with appropriate extract from security policies) including applicable standards for compliance.
* Non-disclosure and confidentiality agreements/clauses.
* Controls to ensure information asset protection:
* applicable procedures to protect Microlink’s information and other information assets (hardware, software)
* controls to protect against malicious software
* any restrictions on the copying and disclosing of Information.
* Access control policy, covering:
* permitted access methods
* the control and use of User IDs and passwords
* an authorisation process for user access
* a requirement to maintain a current list of individuals authorised to have access including their rights and privileges with respect to such access
* a description of services to be made available, including dates, times, and contingency arrangements
* a process for revoking access rights
* measures to ensure the return or destruction of information and equipment at the end of, or at an agreed point of time during, the Contract.
* Applicable change management procedures.
* Arrangements for Incident management reporting, in the event of loss or compromise of Microlink information.
* Intellectual property rights (IPR) and copyright assignment and protection of any collaborative work.
* Service Level Agreements.
* The right to monitor and revoke any activity related to information and information assets.
* Microlink’s right to audit, including the ability to have such audits performed by an independent third party.
* The establishment of escalation processes for problem resolution or arbitration.
* The respective liabilities of the parties to the agreement.
* The implications for Business Continuity and Disaster Recovery.
* Responsibility for legal compliance (e.g. Data Protection Act), including different national legal systems where the Contract involves co-operation with organisations in other countries.

# Third Party Service Delivery Management

It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

Microlink must ensure that delivery of services by Third Parties is in accordance with appropriate service level agreements including any requirement for the delivery of any security arrangements.

Contracts with third parties must be monitored for adherence.

# Monitoring Third Party Services

The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.

Microlink will nominate an individual to liaise with appropriate third parties to ensure that services are being operated in accordance with service level agreements and that any security incidents are reported in a timely manner.

The nominated representative should consider the following:

* monitoring the service level performance
* review of appropriate service reports provided by the third party
* arrangement of regular meetings to discuss service agreements, performance, adopting of Microlink’s relevant policies and procedures
* Problem identification and resolution including any disputes.

As part of the information security schedule, all third party services will be subject to the following:

* An annual risk assessment of services provided.

Changes to Microlink’s information systems by third parties must adopt Microlink’s change management process. The Head of IT must address any changes to services and the security consequences of such changes.

# Security Policy Requirements

Microlink’s Security Policies are to be followed by all third parties. These policies set out the security measures to be implemented and maintained by Microlink in relation to all aspects of information security and all associated supporting processes. They determine the minimum level of security to be achieved by the third party in relation to Microlink business.

These main policy statements are the fundamental principles of security. All aspects of security within Microlink are intended to support these principles.

All third parties must ensure that they do not breach any of the information security management system statements at any time during their contract with Microlink.

# Staff Screening

Confirmation of identity and qualifications of permanent, temporary or contract staff, when requiring access to Microlink buildings, systems and information, is the responsibility of all third parties. In addition, the third party is responsible for ensuring that all permanent, temporary or contract staff sign a confidentiality agreement that protects the confidentially of Microlink information.

Microlink reserves the right to request that third parties provide the appropriate evidence to show that the activities have been undertaken and also occasionally audit to verify that adequate checks are taking place.

# Access to Microlink Information and Information Systems

Any compromise to the confidentiality, integrity or availability of Microlink’s network or systems, could gravely impair the ability to support business.

Access to any of Microlink’s Systems and facilities by Third Parties shall not be provided until the Compliance Manager has granted approval for connection. This will be based upon a formal RA as detailed above.

All physical access to processing facilities shall be monitored and reviewed for compliance against all relevant Policies and Standards at a period of normally 12 months as part of the Information Security Review Schedule, unless required more frequently due to high risks, security incidents or issues of non-conformance.

# Electronic Access

When establishing logical access the following must be applied:

* Access to Microlink’s information, information systems and networks, shall be granted only to those third parties that have formally agreed to comply with the policies and having signed a confidentiality agreement.
* Access must be granted on the ‘need to know’ principle, with access to systems and applications that they require to fulfil their duties.
* Access to information and information systems will be authorised by the relevant System Owner where there is a clearly defined business need.
* The access provided shall always limit the third party to the agreed method of access, the agreed access rights and the agreed level of functionality.
* Each user / Third Party shall be assigned a unique User ID and password. Only the assigned user may use that User ID and use only their User ID for access.
* Third Parties are responsible for maintaining the confidentiality of passwords. Users must not divulge their password to any other person under any circumstances and must not write them down.
* All third parties must inform Microlink when access is no longer required and the system owner must revoke access when it is no longer required.
* Microlink will be responsible for periodically reviewing all third party access rights and formally checking and amending access. This will be completed at intervals not exceeding six months.

# Network Access Control

All remote connections to Microlink’s system from remote servers and applications outside Microlink’s environment, including Internet connections, must be authorised by the Head of IT. An appropriate risk assessment must be conducted before activating the connectivity.

Before allowing connections to a third party system, the owner must ensure that it is adequately secure. Microlink reserves the right to audit the security measures in place on the third party connected systems.

All physical connections to external networks must be secured using a Firewall or other appropriate network security device approved by the IT Manager.

# Anti-Virus Management

All workstations, desktop computers and servers with access to Microlink network must be installed with appropriate antivirus software; the antivirus must be active at all times when the system (laptop, worktop, server) is switched on and kept up to date. This also applies to all third parties owned equipment.

The responsibility for the provision of Antivirus measures for Microlink’s owned assets would be clearly established and documented in third party contracts.

Laptop users and third party staff who use PCs for work off-site must be supplied with virus detection software and regular updates. Such staffs are responsible for installing and maintaining their virus detection software.

Any employee or third party who attempts to disable, defeat or circumvent applicable security controls will be subject to immediate dismissal or contract termination.

All virus outbreaks infecting Microlink’s environment must be reported immediately to the IT Manager & copied to Information Security Manager.

Any machine that might be infected by a virus must be disconnected immediately from all Microlink networks. Infected machines may not be reconnected to the network until security administrators can verify that the virus has been removed.

# Security Incident Management

All third parties are required to report any potential or actual breach of security affecting Microlink’s information or information systems. A breach of security is unauthorised access to premises, information and information systems.

Examples of possible security incidents include:

* loss or theft of computer equipment
* inappropriate use of the Internet
* unauthorised access to a Microlink system
* virus outbreak.

Any third party who becomes aware of a security breach or attempted breach of Microlink’s Information or Information systems must report it immediately to the System Owner and copied to the Information Security Manager or designated security personnel.

All third parties are required to report any breaches of information security within their own organisations, to ensure that any risk to Microlink’s information arising from the third party’s breach can be investigation and managed by Microlink personnel.

Microlink will investigate all security breaches.

The Information Security Manager will collate information about security incidents, and trends analysed, so that further controls can be implemented if required.

# Information Confidentiality

All third parties are required to handle Microlink information in accordance with the Information Classification and Handling Policy. In particular, personnel shall not disclose or discuss Microlink information to any non-permanent employee, or contractor or third party without explicit authorisation from Microlink.

All third parties will sign general confidentiality and non-disclosure agreements integrated within their contract with Microlink

All information developed by or on behalf of Microlink will remain the property of Microlink and shall in no way be sold, copied or used without the express permission of Microlink or authorised designate.

# Media and Paper Document Handling

All third parties are to create all Microlink documents and files under version control and adhere to Microlink’s Documentation and Document Control Procedure and a clear screen and desk policy to protect Information from loss, unauthorised disclosure and loss of integrity. Where appropriate the document should also contain its security classification.

All magnetic media used for such storage shall be clearly labelled; this includes but is not limited to backup tapes, CD’s and memory sticks.

All magnetic media containing Microlink’s information classified as ‘Confidential’ that is transported off-site must be encrypted using an appropriate data encryption product or password protected and stored in a suitable container. Magnetic media that is to be posted should be put into a suitable disk mailer envelope and then into a padded envelope. For urgent transportation of all magnetic media containing Microlink information classified as “Confidential” a reputable courier company must be used.

All paper copies containing Microlink information classified as “Confidential” must be carried in clearly marked slips marked as “Confidential” at all times. Should they be posted a reputable courier must be used and be hand delivered to the individual marked as recipient.

## Disposal of Microlink Media

Media containing Microlink information shall be disposed of securely either by physical destruction of the paper or media or by secure erasure of stored data.

## 18.2 Removal of Property

No equipment (hardware or software) shall be removed from Microlink’s premises by a third party without prior written authorisation from appropriate Microlink personnel.

Any proposed removal or change to equipment will be subject to change control.

# Clear Desk and Clear Screen

A Clear Desk Policy will be adopted for all third parties encountering Microlink information. Documents will not be left unattended or in a position where they may be overlooked by unauthorised personnel. Similarly, computer screens will not be situated or positioned so that Microlink information can be overlooked.

If the work area is left unattended for any length of time Microlink paperwork or storage media containing information must be put away to prevent others from reading, copying or removing it. To prevent unauthorised access to Microlink information on computer systems the third party will log off the computer.

# Use of Microlink Email and Internet Services

All electronic mail messages composed, sent or received using Microlink systems remain the property of Microlink.

Material that could be considered offensive (racial, sexual, religious), defamatory, obscene, pornographic, threatening, abusive or otherwise inappropriate must not be accessed, viewed, downloaded, uploaded, copied, stored, printed or transmitted using Microlink computer systems.

Systems provided by Microlink are to be used solely for business purposes.

# Change Control

The Head of IT must approve modifications, upgrades and new installations of software and hardware to the Microlink network by a third party.

All changes to the configuration of Microlink servers must be recorded as part of the company business continuity plan. Only the IT Team is permitted to install hardware and software.

# Audit & Monitoring

Microlink has deployed comprehensive security systems with the capability of monitoring and recording all Internet and e-mail usage.

Microlink reserves the right to monitor and intercept any e-mail and Internet activity over its network for any of the following reasons:

* record keeping purposes
* checking compliance with regulations and appropriate internal policy
* quality control or staff training
* preventing or detecting crime
* investigating or detecting the unauthorised use of e-mail
* checking for viruses or other threats to the system.

In addition, Microlink’s IT personnel have the ability to inspect any information processed and stored on the network or local disk storage by third parties.

# Compliance

## 23.1 Policy Compliance

The Microlink Board expect that all personnel will achieve compliance to the directives presented within this policy.

This policy will be included within the Internal Audit Programme, and compliance checks will take place to review the effectiveness of its implementation.

## 23.2 Exceptions

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question:

* If complying with the policy would lead to physical harm or injury to a member of staff.
* If complying with the policy would cause significant damage to the company’s reputation or ability to operate.
* If an emergency arises.

In such cases, the staff member concerned must take the following actions:

* Ensure that a manager at Microlink is aware of the situation and the action to be taken.
* Ensure that the situation and the actions taken are recorded in as much detail as possible on an Incident Report.
* Ensure that the situation is reported to the Information Security Manager as soon as possible.

In addition, the Information Security Manager maintains a list of known exceptions and incidents. This list contains:

* known breaches that are in the process of being rectified
* minor breaches that are not considered to be worth rectifying
* any situations to which the policy is not considered applicable.

Microlink will take no disciplinary action in relation to known, authorised exceptions to the information security management system.

## 23.3 Penalties

Non-compliance is defined as any one or more of the following:

* Any breach of policy statements or controls listed in this policy.
* Unauthorised disclosure or viewing of confidential data or information belonging to Microlink.
* Unauthorised changes to information, software or operating systems.
* The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body.
* The exposure of Microlink to actual or potential monetary or reputable loss through any compromise of security.
* Any person who knows of or suspects a breach of this policy must report the facts immediately to the Information Security Manager or Senior Management.

Any violation or non-compliance with this policy may be treated as serious misconduct.

Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.

# Review

This policy shall be reviewed at least annually by the Legal and Compliance Team to ensure continued compliance with regulations, and to ensure the document remains up-to-date with current company practices.

# Signature

This policy is signed and approved by Legal Counsel.



Signature:

Name: Michael Moore

Position: Legal Counsel

Date: 19.11.2024