Microlink Security Policy

Version history

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Amended By** | **Summary of Change** | **File Location** | **Approved by/ Date** |
| 0.1  | 20/04/2018 | ISM | Initial document prior to approval   |  network |  MD |
| 1.0 | 01/05/2018 | ISM  | After approval |  network |  MD |
| 1.1 | 01/05/2019 | ISM | Reviewed with no changes. | network | MD |
| 1.2 | 26/11/2020 | ISM | Reviewed with no changes. Document format updated | Intranet | MD |
| 1.3 | 07/12/2021 | ISM | Reviewed with no changes | Intranet | MD |
| 1.4 | 07/12/2022 | ISM | Reviewed with no changes | Intranet | MD |
| 1.5 | 24/01/2024 | ISM | Reviewed with no changes | Intranet | MD |
| 1.6 | 06/12/2024 | ISM | Reviewed with no changes | Intranet | MD |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Contents

[1 Introduction 3](#_Toc187144509)

[2 Aim and Scope of this policy 3](#_Toc187144510)

[3 Responsibilities 4](#_Toc187144511)

[4 Legislation 4](#_Toc187144512)

[5 Personnel Security 5](#_Toc187144513)

[6 Asset Management 5](#_Toc187144514)

[7 Risk Management 5](#_Toc187144515)

[8 Boundary firewalls and internet gateways 6](#_Toc187144516)

[9 Secure configuration 6](#_Toc187144517)

[10 User access control 6](#_Toc187144518)

[11 Malware protection 7](#_Toc187144519)

[12 Software and firmware Patch management 7](#_Toc187144520)

[13 Secure Back-up 8](#_Toc187144521)

[14 Mobile Working 8](#_Toc187144522)

[15 Public Website and Social Media 8](#_Toc187144523)

[16 Physical and Environmental Management 8](#_Toc187144524)

[17 External Services 9](#_Toc187144525)

[18 Information security incidents 9](#_Toc187144526)

[19 Reporting 9](#_Toc187144527)

[20 Further Information 9](#_Toc187144528)

# Introduction

This security policy document is part of a set of policy documents that together represent the policy of the Microlink Organisational approach to security. Therefore, this policy should be read in connection with the policies and procedures listed in Table 1.

 Table 1

Related Policies and Procedures

|  |  |
| --- | --- |
| Title  | Version  |
| Microlink HR Policy and Procedures  | 2022 |
| Microlink Data subject Access request procedures  | 5.1 |
| Microlink Security Procedures  | 2.4 |
| Microlink Business Continuity and Disaster Recovery Plans  | 3.0 |
| Microlink Privacy policy and procedures for clients  | 5.0 |
| Microlink Data Protection Policy and Procedures  | 4.2 |
| Microlink Data breach and Information security Incidence Reporting Procedures  | 3.2 |
| IAMS IT Operations Manual  | 17.1 |
| Microlink Risk Management policy | 1.0 |

This security policy is a key component of Microlink management framework. It sets the requirements and responsibilities for maintaining the security of information within Microlink. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

The security policy and procedures are reviewed Annually. The annual review will also involve consulting the staff.

# Aim and Scope of this policy

The aims of this policy and related policies and procedures (see Table 1) are to set out the rules governing the secure management of our information assets by:

* preserving the **confidentiality, integrity and availability** of our business information
* ensuring that all members of staff are aware of and fully comply with the relevant **legislation** as described in this and other policies.
* ensuring an approach to security in which all members of staff fully understand their own **responsibilities.**
* creating and maintaining within the organisation a level of **awareness** of the need for information
* detailing how to **protect** the information assets under our control.

This policy applies to all information/data, information systems, networks, applications, locations and staff of Microlink or supplied under contract to it.

# Responsibilities

Ultimate responsibility for information security rests with the Managing Director of Microlink, but on a day-to-day basis the **Information Security Manager** shall be responsible for managing and implementing the policy and related procedures.

 Responsibility for maintaining this Policy, the business information Risk Register and for recommending appropriate risk management measures is held by the **Information Security Manager.** Both the Policy and the Risk Register shall be reviewed by the **Information Security Manager** at least annually.

**Line Managers** are responsible for ensuring that their permanent staff, temporary staff and contractors are aware of:

* The information security policies applicable in their work areas
* Their personal responsibilities for information security
* How to access advice on information security matters

**Line managers** shall be individually responsible for the security of information within their business area.

**All staff** shall comply with the information security policy and must understand their responsibilities to protect the company’s data. Failure to do so may result in disciplinary action.

* Each member of staff shall be responsible for the operational security of the information systems they use.
* Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

**External Parties**: Access to the organisation’s information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place.

* Such a contract shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

# Legislation

Microlink is required to abide by certain UK, European Union and international legislation. It also may be required to comply to certain industry rules and regulations.

The requirement to comply with legislation shall be devolved to employees and agents of Microlink, who may be held personally accountable for any breaches of information security for which they are responsible.

In particular, Microlink is required to comply with:

* The Data Protection Act (2018)
* The Data Protection (Processing of Sensitive Personal Data) Order 2000.
* The Copyright, Designs and Patents Act (1988)
* The Computer Misuse Act (1990)
* The Health and Safety at Work Act (1974)
* Human Rights Act (1998)
* Regulation of Investigatory Powers Act 2000
* Freedom of Information Act 2000
* Equality Act 2010

# Personnel Security

People are an important asset of any organisation. It is important that from as early on as the recruitment phase, security requirements are considered for all staff. That qualifications are checked, and references are taken. That contracts contain a security and confidentiality clause. That staff receive appropriate induction and ongoing training. That staff understand what is expected of them.

**Personnel Security is that staff are recruited, inducted, receive regular training and are made aware of their responsibilities as appropriate to their position.**

# Asset Management

Identifying the physical and information assets of the origination is a first step in introducing a risk assessment and applying appropriate security controls. As the risk assessment is a yearly activity, it is essential that accurate records are kept, of source ownership, modification and disposal. An asset is any hardware, software, application or data used to fulfil the origination’s function.

**Asset Management is that a record of all physical and software assets is to be maintained, and all particularly valuable or sensitive information assets shall be identified through the use of data classification. (Refer to 2. Asset Management in Microlink Security Procedure for more information)**

# Risk Management

The board has established an appropriate culture to promote and monitor the management of risk. The purpose of risk management is to identify, evaluate, monitor, manage and report financial, reputational and other risks faced by the organisation- at both a strategic and an operational level. Thereby adapting a legal compliance as a minimum standard to maintain a robust system of internal controls to safeguard the organisation’s investments and assets.

A risk assessment must be carried out against all assets. The aim of a risk assessment is to establish the liability to Microlink of a threat being successfully exploiting a vulnerability.

**The risk management is that a risk analysis is to be carried out on a regular basis (at least once a year) and the risk assessment is to form part of the yearly security review by the board. (Refer to 3. Risk Assessment in Microlink Security Procedure for more information)**

# Boundary firewalls and internet gateways

A boundary firewall can protect against commodity cyber threats by restricting inbound and outbound network traffic to authorised connections. Such restrictions are achieved by applying configuration settings known as Access control rules or firewall rules. An incorrectly configured boundary firewall (or internet gateway) can give access to the organisation’s network exposing the organisation to a cyber-attack and unauthorised access to the information contain on the network.

 **The Boundary Firewalls and Internet Gateways is to ensure that Information, applications and computers within the organisation’s internal networks should be protected against unauthorised access and disclosure from the internet, using as boundary firewalls and internet gateways. (Refer to 4. Boundary firewalls and internet gateways in Microlink Security Procedure for more information)**

**A weekly vulnerability scan of all external IP addresses should be carried out by a suitable external company, and act on the recommendations, reflecting the change in the risk assessment and security policies.**

# Secure configuration

Default installations of computers and network devices by their very nature aim for a quick install, often including an administrative account with a predetermined, publicly known default password, one or more unnecessary user accounts enabled. This leaves the many open channels through which cyber attackers are given a variety of opportunities to gain unauthorised access to an organisation’s sensitive information. By hardening the system, we can prevent commodity cyber-attacks.

**The Secure Configuration is that computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role. (Refer to 5. Secure configuration in Microlink Security Procedure for more information)**

# User access control

Cyber attackers target those accounts that will give them the greatest level of access to information, applications and systems, especially privileged accounts such as administrative accounts; typically have the greatest level of access to information, applications and computers.

When a privileged account is compromised an attacker can exploit this privilege to access other systems, resulting in large scale corruption of information and affect the business processes across an organisation.

To protect the organisation’s system, the principles of least privilege and separation of concerns should be applied to user accounts: limiting the privileges granted and restricting access.

**The User Access Control is that all user accounts should be designed only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks. This applies to all user accounts put especially those accounts with special access privileges. (Refer to 6. User access control in Microlink Security Procedure for more information). The user access is that a separation of concerns and a less privilege approach is taken to user access.**

# Malware protection

Computers can be infected with malware through various means. However, the common method is through users opening an affected file, email attachment, browsing a compromised website or opens an unknown file on a removable storage media.

Computers are particularly vulnerable to malicious software when exposed to the internet, this includes desktop PCs, laptops and mobile devices. Hence, when available dedicated software is required that will monitor for, detect and disable malware.

**The Malware Protection means computers that are able to connect to the internet or connected to devices that are connected to the internet, should be protected against malware infection through the use of malware protection software. (Refer to 7. Malware protection in Microlink Security Procedure for more information)**

# Software and firmware Patch management

Any software can contain technical vulnerabilities (weaknesses, flaws, bugs etc). Vulnerabilities are common in all types of popular software. When discovered and once known, they can quickly be deliberately exploited by malicious individuals or groups to attack an organisation’s computers and networks. Software vendors will try to provide fixes for identified vulnerabilities as soon as possible, in the form of software updates (patches). The vendor will release the patches to their customers, this may be through a formal release schedule. By doing this, they also let everyone else know that there is a vulnerability in the software. Hence to avoid becoming a victim of a cyber-attack that exploit the software vulnerabilities, an organisation needs to manage patches and the update of software effectively.

**The Patch Management is that Software running on computers and network devices should be kept up-to-date and have the latest security patches installed. (Refer to 8.**

**Software and firmware patch Management in Microlink Security Procedure for more information)**

# Secure Back-up

An essential component of the business continuity plan is secure back-up.

**The back-up is that regular secure back-ups of data are undertaken and restored tested at appropriate intervals. (Refer to 9. Secure back-up in Microlink Security Procedure for more information)**

# Mobile Working

Staff will need to, from time-to-time, work outside the office on mobile devises (laptops, tablets and phones), these devices need to follow the same security protocols as any other company device, whether in the office or on the road. The same policies apply to whether the device is supplied by the organisation or is a personal device used also for business.

**The mobile working is that all devices are subject to approval and securely configured. (Refer to 10. Mobile working in Microlink Security Procedure for more information)**

# Public Website and Social Media

Social media is an important aspect of the marketing of an organisation, given social media’s ability to influence a large number of potential customers. It is necessary that access to the origination’s social media accounts are secured appropriately. Similarly, our websites are representing our brand image and therefore we do not want to be misrepresented by a cyber-attack.

**Public websites and social media accounts is that they are protected in a similar way to other sensitive accounts. (Refer to 11. Public Website and social media in Microlink Security Procedure for more information)**

# Physical and Environmental Management

Environment management of physical equipment is an important aspect to ensure that it continues to operate effectively. In addition, physical security is necessary to ensure equipment is not damaged to tampered with and thereby expose assess to loss or damage.

**Physical and Environmental Management is that all physical equipment shall be protected from physical threats and environmental hazards. (Refer to 12. Physical and Environment Management in Microlink Security Procedure for more information)**

# External Services

In modern information systems it is sometimes cost effective to use services provided by a third party, such as payroll, HR, cloud-based service, etc. So as such these services need to provide the same level of or better procedures for data confidentiality, integrity and availability for our information assets.

**External services are that they must demonstrate that they are providing the same level of security for our assets as described in this policy. (Refer to 13. External service providers in Microlink Security Procedure for more information)**

# Information security incidents

It is important to ensure that all security incidences are investigated properly. This includes all breaches of the security (this) policy, losing a mobile device and all other information security incidents. The staff require a clear set of procedures when reporting and investigating any security incidence. The lessons learnt from any incident investigation should be reviewed and if necessary, to include in the risk assessment.

**Data breach and Information security incident policy is that all incidents should be logged and investigated to establish their cause and impact with a view to avoiding similar events.**

# Reporting

The Information Security Manager shall keep the business informed of the information security status of the organisation by means of regular reports to senior management.

# Further Information

Further information and guidance on this policy can be obtained from Information Security Manager. Comments and suggestions to improve security are always welcome.