Application Security Policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change | Approved by: |
| 1.0 | 12/06/2019 | David H | Initial publish | David H |
| 2.0 | 30/09/2022 | David H | Added Version history and document owner |  |

**Document Owner HR and Legal**

# Introduction

Applications are at the heart of any IT environment. Without them there would be no need for the environment in the first place. Everything you do on a computer is done through installed application whether its Accounting packages for finance management, Office packages to improve productivity, remote support tools for when you need help, or web browser for connecting to CRM systems. The width a breadth of functionality is limitless.   
Although most software application are legitimate and work well, some software can be written poorly introducing security vulnerabilities, system instability or impact system performance.   
Whilst other software can be written with malicious intent such as to acquire personal information via malware and keyloggers or written to Lock you out of your data by maliciously encrypting it via ransomware. Whilst we want to take advantage of great software applications that bring value, and even revenue streams into the business. We need to avoid malicious and poorly written software, ensure software is safe and does not introduce viruses and other malicious code, ensure the software is used in an acceptable way.   
Compounding matters is how readily available software is online,  
Ensuring we have the correct controls are in place to protect the organisation IT environment is more important now than ever before.

# Policy Objectives

* 1. The Application Security Policy sets out to aid in protecting the IT environment from threats such as computer viruses, malicious code, violation of privacy and interruptions to service that can be introduced with the implementation/installation of software applications.
  2. The policy seeks lay down the minimum-security standard applicable to software applications used within Microlink.

# Definitions

|  |  |
| --- | --- |
| **Standard applications:** | A standard application is one that is included as part of the standard deployment environment. |
| **Non-standard application:** | This is any software application that is manually installed and not part of standard deployment environment. |
| **Unauthorised software:** | Unauthorised software includes any item of software that is installed on any device within the organisation without the prior knowledge of the IT team. This includes Trojans, Viruses, games, freeware, shareware, or any software that promotes hacking, system intrusion or system performance degradation. |
|  |  |
|  |  |

# Scope

* 1. The Application Security policy applies to all Information Technology systems and components there of specifically
* Server and other devices that provide centralised computing capabilities.
* SAN, NAS and other devices that provide centralised storage capabilities.
* Desktop workstations, Laptops and other devices that provide distributed computing capabilities.
* Routers, switches, and other devices that provide network capabilities.
* Firewalls and other devices that provide dedicated security capabilities.

# Policy restrictions

## Control of applications

Due to the variety and how readily available software applications are, a measure of control over what application can run and execute in the environment will be required.  
This will ensure continuity of service. Security, performance, and availability may become compromised due to the introduction of non-standard or unauthorised applications.

* + 1. Internal IT shall evaluate all new application to determine their suitability for installation to the IT environment. Any application that is does not pass the evaluation will be rejected and therefore not installed into the IT environment.
    2. Controls should be in place to only allow authorised list of software applications from running.
    3. Microlink reserves the right to remove and piece of software or application that is deemed unsuitable to the environment.
    4. The installation of unauthorised software is NOT permitted on any server or workstation.
    5. Internal IT will maintain and audit a software inventory and identify and investigate any unauthorised software found.
    6. All software licenses introduced to the IT environment should be maintained in a list by Internal IT
    7. To ensure legal compliancy, only fully Licensed software, where licenses are applicable, will be installed into the IT environment.

## Application level Authentication.

Some applications require their own authentication within the application itself. This poses an issue, increasing the number of authentication databases where credentials are stored. Avoiding using embedded authentication databases reduces the number of locations that credentials are stored.   
This in turn reduces the threat attack service (less systems to hack), maintenance, administrative tasks all whilst ensuring continuity of credential security across systems, (password strength and complexity) and improves user experience, Single Sign On means users do not have to remember multiple password reducing the temptation to write them down. Further indirectly increasing security.

* + 1. As Microlink employs Active Directory Domain Services (ADDS). Wherever possible application should be configured to integrate with ADDS for authentication. Integrations include:
       1. Lightweight Active directory protocol (LDAP)
       2. Active Directory Federated services. (ADFS)
    2. Where embedded authentication databases are required
       1. Default database passwords/accounts should be changed before being introduced to production environment or on first use and stored in compliance with password policy.
       2. Passwords must comply with password complexity defined in the password policy.
       3. Unique secrets (passwords) must be used for each application.
       4. Where possible unique identifiers (username) should be used.
       5. Access to the installation and application files should be controlled.

## Application Approval

As a minimum and to avoid introduction of malware, trojans, virus etc and to ensure installation media has not been tampered with.

* + 1. Application installation media or packages must be scanned for viruses prior to be installed or executed.
    2. Where possible Installation media must have a file, hash checked against one provided by the software vendor. This is to ensure integrity of the installation media.
    3. Applications must be sourced directly from software vendor or approved supplier website or supplied via a contact of the software vendor or approve suppler.

## Application service accounts

Some applications will require an OS service account, application logon account or OS logon account. These accounts must be subject to the same rules as standard operating accounts.

* + 1. Group/Managed Service Accounts (gMSA) should be used where possible.
    2. All non MSA /gMSA accounts are required to have addition password complexity and additional controls may be required.
    3. All accounts application/service accounts must be granted only those privileges required to correctly operate. This follows the least privilege paradigm.
    4. Where privileged rights are granted to an application account the privileges should be reviewed regularly and removed when no longer required.

## Software maintenance

In certain instances, third party partners may be required to install or maintain software applications. This poses a risk as they will not have as in-depth knowledge of Microlink polices as Microlink employees. This means further controls needs to be in place to ensure work carried out for maintenance is completed in a safe way that does not breech privacy or impact performance.

Software maintenance is also important in maintaining IT security. New patches and updates commonly contain fixes for vulnerabilities previously unknown.

* + 1. Software maintenance by third parties.
       1. Accounts used by third party providers must be granted only those privileges required to correctly operate. This follows the least privilege paradigm.
       2. All third-party account must only be activated when work is to be carried out. And must be disabled or removed when not in use.
       3. Third parties must be actively monitored and supervised to ensure normal operating controls are enforced. Such as restricting the ability to take soft or hard copy data.
    2. Application updates and patches should comply to patch management policy.

# Policy Violations

Any violation of this policy should be brought to the attention of the Head of IT and the Information Security Manager, who will work with the relevant department heads or appropriate individuals to rectify the problem.

# Approval

|  |  |
| --- | --- |
| Name: | [Enter Name here] |
| Position: | [Enter Position Here] |
| Date: | [Enter Date of signing here] |
| Signature: | [Add Signature image here] |