NETWORK SYSTEMS MONITORING POLICY

Introduction

The objective of this Policy is to protect the integrity of the Organisation's information systems by the regular monitoring of network events and consistent updating of software.

Responsibilities

1. The Internal IT Manager is responsible for administrating and updating the individual event log monitoring procedures as necessary.
2. The Head of Operations (ISMS Manager) is responsible for the monitoring duties as required by this Policy, and for escalating Incident Reports without delay to the CEO.

Log monitoring

The Internal IT Manager will arrange for the following to be monitored on a daily basis:

1. All servers and services are up and working efficiently
2. E-mail is working.

The Internal IT Manager will arrange for the following to be monitored on a regular basis:

1. All Server event logs
2. Antivirus logs
3. Firewall event logs.

When a serious event is noted, it must be escalated to the Head of Operations (ISMS Manager).

Security Patches/Updates

As new threats are constantly appearing, it is essential that the Organisation's defences are kept up to date.

Security patches and operating system updates available from the Software providers are checked for usability prior to installation, when applicable.

The Internal IT Manager is responsible for arranging the installation of updates and patches as they are issued.

Updating of antivirus software is automatic and is covered in the Virus Protection Policy.

Policy Sign-off

Date of Issue:	27/10/2020
Date of Next Review:	30/09/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	30/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Updating responsibilities and date