Malware Protection Policy

1 Purpose

This document provides detailed policies that govern the operation and use of software specifically designed to protect WELDO connected systems from malicious software.

2 Scope

This policy aims to set out malware and anti-virus policy within WELDO. This policy applies to all WELDO staff authorized to use/access IT systems and communications networks whether they are employed directly by WELDO, customer organizations, contractors, voluntary organizations or suppliers granted access for support purposes.

3 Policy

Configuration Standards

3.1 Approved Anti-virus software MUST be correctly installed and configured on all supported endpoint and servers across WELDO network to the following configuration standards Anti-virus software MUST be kept up to date including the definitions files.

3.2 Anti-virus software updates MUST be deployed across the network automatically following their receipt from the vendor and it must be configured to check for these updates every 24 hours.

3.3 Anti-virus software MUST be configured for real time scanning and regular scheduled scans.

3.4 On-access scanning MUST be configured within Anti-virus software for removable media and websites.

Anti-virus server MUST be monitored on a daily basis by a IT Manager and DPO for virus alerts.

In the event of a virus infection which infects multiple devices (more than 3 devices) at the same time. A root cause analysis report should be completed by the DPO.

Monthly Anti-Virus compliance reports MUST be provided to the DPO.

Tamper protection MUST be enabled to prevent end users or malware altering the antivirus software's configuration or disabling the protection **User Responsibilities**

3.5 All IT equipment and removable media MUST be scanned for viruses and malware before being introduced or prior use on the corporate network, system or device

3.6 Users MUST not accept, or run, software from non-trusted sources

3.7 Users must not undertake any activities with the intention to create and/or distribute malicious programs (e.g. viruses, worms, Trojans, e-mail bombs, etc) into corporate network(s) or system(s)

3.8 Users MUST inform the IT Manager immediately if a virus is detected on their system.

3.9 IT system(s) infected with a malware/virus that the anti-virus software has not been able to deal with MUST be disconnected/quarantined from the organizational network until virus free