Service Bulletin

Return/Repair Policy on Potentially Compromised Equipment

Compromised Equipment

Customers must recognize any issues due to unauthorized installation of third party software, viruses, malware, modification or alteration of software or hardware, or misuse are not covered under warranty.

If a device is suspected to contain any potential virus or malware Monroe Electronics/ Digital Alert Systems (the company) will not attempt to diagnose or reformat the storage media. If a repair is requested, the company will replace the storage media at customer expense with a new storage device.
Further, if the company has reason to believe equipment returned for evaluation is compromised with viruses, malware or other security issues, the company will advise the customer and replace the storage media at customer expense.

There is no warranty for loss of, or damage to data— as a matter of practice all logs and configurations should be regularly backed up to a separate storage device. However, be aware the backup storage device(s) may also be compromised, and the company is not liable for any viruses or malware that may transfer from compromised equipment to a separate storage product or other networked devices.

A reminder on computer and network security

It is the user's responsibility to maintain this equipment in a secure operating environment. Monroe Electronics will have no liability for loss of equipment, data, or loss of use of system(s) arising out of improper usage of this equipment, including but not limited to the failure to maintain this equipment in a secure network operating environment.

Always protect equipment behind a firewall

Restricting access to EAS (and any other computing) equipment through firewalls and other network layer controls to only trusted IP addresses may reduce external security risks to your equipment. In all cases, users should implement architectures to restrict access to its EAS equipment, using methods such as strong firewalls, demilitarized zones (DMZ), or virtual private networks (VPNs). It is important to design the network optimally such that a firewall is positioned to inspect all incoming or outgoing network traffic.

Change your default passwords, and regularly check for software updates.

Users must change their default (factory supplied) passwords, and utilize strong passwords for all user accounts. Users should also ensure that software updates are applied in a timely manner.

Customers are encouraged to read the company's white paper: *Understanding Security for Your EAS Equipment – Best Practices and Recommendations for Users* available on our websites at:

Monroe Electronics:
http://www.monroe-electronics.com/EAS_pages/pdf/ME%20EAS%20Security%20WhitePaper%2001152014.pdf

Digital Alert Systems
http://www.digitalalertsystems.com/pdf/DAS%20EAS%20Security%20WhitePaper%2001152014.pdf

Revision: 1.1 Publication: SBMEDAS-1016

Electrostatic Measurement
Emergency Alert Systems
CATV Switching and Control

585-765-2254 fax 585-765-9330
100 Housel Ave. | Lyndonville | NY | 14098
www.monroe-electronics.com
www.digitalalertsystems.com