NIHON KOHDEN CORPORATION

June 8, 2017

Dear Customers (responsible for facility),

How To Defend Against Ransomware*

We hereby notify the impact and action to our devices against ransomware (a type of malware) which has been widely publicized since the middle of May, 2017.

1. **Impact on our devices**
   We are investigating followings.
   (1) Possibility of infection on our devices
   (2) Assumed malfunction when infected
   (3) How to address when infected
   We will let you know results upon completing the investigation.

2. **Preventive action at customer**
   Isolating devices from the source of ransomware, updating the system software and device application software to be invulnerable are required to avoid being infected. We are working on the latter by inspecting devices with updated Windows and by updating device application software. We recommend customers to take action for the former as shown below.
   (1) If your devices are connected to network and its operator's manual or related document requires you to disconnect from external network, make sure again that your devices follow requirements.
   (2) When a PC is included in devices, do not connect other device such as USB memory to the PC since it may contain malware. But if connecting them is absolutely necessary, be sure to check them to see if they are not infected prior to connection.

3. **When you find abnormality**
   When you encounter this threat, or you find any abnormal device operation which seems different from routine operation, immediately notify your distributor of abnormality. Distributor's sales/service staff will take an appropriate action. Action to be taken depends on operating status of devices.

Your cooperation is highly appreciated.

*: Ransomeware is malware known as Wanna Cryptor, WannaCrypt, WannaCry, WannaCryptor, Wcry which prevents users from accessing their files by encrypting, and forces users to pay the ransom to decrypt files.