NIHON KOHDEN CORPORATION

June 8, 2017

Dear Customers (system administrator),

How To Defend Against Ransomeware "WannaCry"

We hereby notify the impact and action to our devices against ransomeware.

1. **Ransomeware "WannaCry"**
   Ransomeware "WannaCry" is malware attacks Microsoft Windows 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. See "Microsoft Malware Protection Center" [*1] for more information.

2. **Impact on our devices**
   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.

3. **Preventive action at customer**
   Microsoft has been providing security patch by Windows Update to be invulnerable. Our engineering division and cyber-security division are working on inspecting our devices closely with updated Windows. Also engineering division has been updating device application software to reflect the result of inspection. Device application software in some products is already updated.

   We recommend customers one of Windows Update (applying MS17-010) and disabling SMBv1 to keep your system protected and to be invulnerable for ransomeware and other malware.

Your cooperation is highly appreciated.

Please refer related site listed below;

Microsoft Security Bulletin MS17-010 - Critical
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

How to verify that MS17-010 is installed
https://support.microsoft.com/en-us/help/4023262/how-to-verify-that-ms17-010-is-installed

How to enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server
https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows-server

*1: https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx