

WMS & NIC INFORMATIONAL SHEETS

All Clients with Servers need to be PCI-DSS, HIPPA and/or Sarbanes-Oxley Compliant. At WARD Computers, we offer the **WMS (WARD Computers Managed Services)**. This is a Server monitoring service by WARD Computers that helps keep your Server and network in compliance and running their best.

With your subscription to the WMS program, WARD Computers technicians will remote into your network, on a set schedule, to keep your Server (including Dinerware Brain, RMS Data Server, or any data server) backups, network, and In-House software (Dentrix, Dinnerware, RMS etc.) up to date and secure.

PCI compliance laws state that any server in which customer payment information is passed through must pass a PCI Compliance scan once per Quarter. The lack of a single Windows Update can prevent you from passing this scan and result in hours of paperwork as well as delayed credit card processing.

With the WARD Computers **WMS support package**, WARD Computers Technicians will complete the following:

- 24/7 - monitoring of the email alerts setup for your Server.
- Daily - monitor the emails for your off-site backups, provided by WARD Computers, ensuring they are completing.
- Monthly –
 - Install Windows and Common Software (Adobe, JAVA et al) Critical updates to prevent security breaches.
 - Make sure Antivirus and Anti-spyware programs are updated, renewed and scheduled scans are running.
 - Review your on-site backups to be sure they complete. If you use a NAS purchased from WARD Computers, this will be reviewed weekly by email alerts and notifications.
- Quarterly –
 - Scan to be sure devices connected to your Server and networks are supposed to be there and are not “rogue” devices. (Non-approved PC’s, employee installed access points, etc.)
 - Scanning, updating and configuring of your router to keep up with ever changing PCI Compliance Laws. Certain routers are recommended for their specific compliance standards (such as SonicWall and Meraki) which can be purchased from WARD Computers.
 - Check for and install of critical updates for your in-house software (such as Dinerware, RMS et al). Some 3rd party vendors require annual maintenance contracts from the end user to receive patches, updates and fixes, these contracts are the responsibility of the end user business, not WARD Computers.

- Semi-Annually - WARD Computers will run a merchant compliance scan (A more in-depth scan of the PCI Compliance checklist.)

The scans and updates are run during weekend or off hours of your business, to reduce performance issues and be sure no compromises are found.

The PCI Compliance checklist is only a part of the Monitoring Services that WARD Computers provides for its valued customers. The **Network Information Checklist (NIC)** includes the WMS services above as well as adding another layer of protection for your business network.

The NIC service provides all the benefits of the WMS program as well as:

- Monthly – Individual backup routines will have data checked for recoverability, and properly archived to save valuable storage space. This requires network storage (NAS) or external drives, which can be purchased from WARD Computers.
- Quarterly –
 - Server event logs are checked and the proper actions taken to correct any errors that are detected.
- On-Site: Quarterly –
 - Battery Backups are tested quarterly, to ensure brown-out protection.
 - Server RAID drives reviewed for stability.
 - WARD Computers will check for motherboard, BIOS, and hardware driver updates and install as needed on your Server.
- Annually - SRT (Server Recovery Test) are run for each Server. This is via a bare-metal-recovery program (provided by WARD Computers) to ensure that your Server image backups will work if data or full recovery is needed.

Possible FEES IF NOT PCI-COMPLIANT** - Average Costs based on Level 4 Business

- \$8,000 to \$20,000 for examination fee, if breach is suspected.
- \$3 to \$10 per card & \$5,000 to \$50,000 in fines.
- Additional fines based on actual fraudulent use of cards.
- Fines of \$500,000 per data security incident.
- Fines of \$50,000 per day for non-compliance with published standards.
- Liability for all fraud losses incurred from compromised account numbers.
- Liability for the cost of re-issuing cards associated with the compromise.
- Suspension of merchant accounts (this means you cannot credit card payments)

**Information based on data provided by <https://www.pcisecuritystandards.org/> on 10/30/2012