SOFTWARE HARDWARE & SECURITY

Customer understands and agrees that data loss or network failures may occur, whether or not foreseeable, if the Customer fails to maintain proper security for its computer and information system including software and hardware updates. Customer therefore warrants that it will follow software and hardware updates and maintain specific security standards, policies, and procedures set forth below.

(x) Business Grade Anti-Virus Software installed on all Desktops, Laptops and Servers.

(x) On A Daily Basis, Check That 3rd Party Software Updates/Patches Are Installed. This Includes, But Is Not Limited To, Anti-Virus Software, Operating System Updates, Application Patches and Firmware Updates.

(x) All External Network Gateways (Including the Cloud) Are Protected by a Business Grade Firewall with a Comprehensive Security Subscription Including Intrusion Detection.

(x) All Critical Data Is Backed Up On At Least a Daily Basis & The Test Restores of All Back-Ups Are Verified on a Monthly Basis.

(x) All Back-Ups Are Stored in a Secure Location Offsite or in a Fireproof Safe (Minimum 2 Hours).

(x) All Systems (Laptops, Workstations, and Servers) and Devices (Smartphones, USB Drives) Storing Personally Identifiable or Protected Health Information Must be Securely Overwritten or Wiped using an Approved Secure File Deletion Utility or Third Party Company that Maintains Industry Certifications Such As ISO-27001, ISO-14001, ISO-9001 upon Decommission of the Device to Ensure that the Information Cannot be Recovered.

(x) All Portable Devices (Such as Laptops, Tablets and Smartphones) Containing Personally Identifiable or Protected Health Information Must Use Industry-Accepted Full-Disk Encryption Technologies*.

(x) All Removable and Easily Transported Storage Media (Such as USB Drives Or CDS/DVDS) Containing Personally Identifiable or Protected Health Information Must Use Industry-Accepted Encryption Technologies*.

*Industry-Accepted" Means Accepted by the Cryptographic Community.

The customer agrees and understands that if it does not comply with the standards represented above, the MSP will not be held responsible for any data loss or network failures.