**Exhibit D**

**Onboarding Requirements**

*\*All items in italics are strongly recommended*

To ensure your network is setup to provide you the possible best efficiency and peace of mind, work needs to be done and tools put in place to enable the exceptional IT experience you deserve. There are several items we will take care of prior to taking you live with our remote Service Team, and the rest we will continue to work on through the life of your contract. The goal is to make your technology work for you and become a strategic advantage for your business.

# Facilities and Utilities

* *Uninterruptable Power Supplies (UPS) are highly recommended. If utilized, the following is expected:*
	+ *Every UPS must have smart management capabilities*
	+ *All of the following must be plugged into the UPS: all servers, backup appliance, NAS, switches for the network. PoE switches are NOT to be plugged in to the UPS.*
	+ *All of the following must be plugged into the Wattbox, which must be plugged into the UPS: firewall(s), ISP equipment including Cable/DSL, Modem, T1 Smart Jack, etc*
	+ *UPS must be capable and configured to provide power for server that takes the longest to shutdown*

# Network / Infrastructure

* All switches must be managed and should be plugged into the UPS.
	+ If existing switch is unmanaged, it must be replaced within 1 year with a managed switch.
* Remote connection to corporate network.
	+ Users working remotely from corporate owned assets will utilize a supported VPN when connecting to the corporate network.
	+ Users working remotely from non-corporate owned assets must connect to a corporate owned asset inside the network using LogMeIn (license provided).
	+ Remote access eligibility is determined by the business manager and will not be enabled on demand from the user.
	+ Open RDP is not allowed (RDP best practices doc).
* Backup and Disaster Recovery (BDR) – must backup all servers.
	+ Documentation required for local and cloud retention settings as well as backup schedules.
	+ Shadow copies must be disabled after BDR is in place and all other backup solutions must be removed.
* All managed Unified Threat Management (UTM) devices must be assigned to the Collabrance Portal, regardless of where they were purchased. *Service Provider should hold 1 preconfigured UTM device in inventory for emergencies that could support their largest customer.*
* IP phones must be on a separate VLAN with appropriate QoS settings. This will require a managed switch. Printers/Desktops/Servers can be on same network segment.
* Network must utilize Category 5 (or better) cables.
* All domains for one subscriber must be housed with the same registrar and DNS zone files must be under that same registrar.
* Collabrance must be able to change public DNS records.
* Internet service must be delivered via a business class service, typically with an SLA. The minimum up/down from the ISP must be 1.5mbps. ISP must deliver a public, static IP address and the internet must be delivered to the firewall via Ethernet.
* *Label all equipment, including modem, firewall, switch and all servers.*

# Servers

* Servers must meet minimum requirements
	+ Disks must have 20% free space at onboarding (recommend maintaining 10% free at all times). Additionally, the minimum size for C drives is 40GB *(recommend 100GB)*.
	+ RAM requirements are 4GB for Domain Controllers and 8GB for application servers, increasing as the application demands it. All servers (physical and virtual) must meet recommended specifications as published by the OS and application manufacturers.
	+ RAID all new servers must be hardware RAID, Single purpose physical servers should be a minimum of RAID 1 and virtual hosts should be a minimum of a 4 disk, RAID 5 set.
		- * If existing servers are software RAID, upgradecycle will require hardware RAID.
* *C:\ should always be reserved for Operating System only. All applications and data should be moved to other drive letters.*
	+ Operating System must be a version currently supported by manufacturer.
* Intelligent monitoring must be set up for hardware components
	+ SNMP is widely available and should always be installed. Toolsets include HP Insight Manager, Dell OpenManage, Intelligent Platform Management Interface.
	+ *IPMI – this is a purchase option, so must be included in server specs if it will be implemented. Tool sets include iDRAC (Dell) and iLO (HP).*
* Warranty
	+ *It is strongly recommended that all servers have a valid manufactures warranty with a 24 hour parts replacement guarantee.*
* Domain Controller
	+ Every environment must have at least one server to function as local domain controller
	+ PDC Emulator should receive time from an external source. All other domain controllers, member servers and desktops should receive time updates as part of the domain hierarchy.
* Security
	+ All Microsoft Service Packs must be installed during onboarding.
	+ Remote Monitoring agent installed and functioning properly.
	+ Supported Antivirus installed and functional; all other AV products removed; device is infection free.
	+ Server must reboot unassisted, without human intervention.
	+ User Access Control must be disabled.
	+ Active Directory must contain active users, servers and workstations only. Former employees will be retained for 90 days as “disabled”.
	+ Event logs must be reviewed by Collabrance and Service Provider for major issues and a resolution plan agreed upon by all parties.
	+ Active Directory structure must be set up to follow our supported standards.
* Network Setup
	+ Each server must have a static IP address.
	+ DNS aging and scavenging enabled (best practices doc).
	+ No multi-homed servers (across multiple subnets).
	+ Remote Desktop Protocol (RDP) must be enabled on the servers.
* Continuity
	+ Co-located hardware must be located in a commercial data center.
	+ Collabrance Backup Solution in place.
	+ All other backup solutions must be disabled (including shadow copies).
* Virtualization
	+ The hardware specifications of the host must meet or exceed the aggregate requirements of all the guests.
	+ *Host server is only a host, it should have no other roles, functions or applications.*
	+ *Hyper-V and VMware management tools should be installed on separate, physical machines that are not powered off.*
* *Major functions (Domain Control, Exchange, SQL) should always be housed on separate servers and this is the upgrade expectation. Servers in place should be evaluated by Collabrance to determine risk of server overload and poor user experience.*

# Workstations and Peripherals

* Workstations must meet minimum requirements
	+ Operating System Professional Microsoft Windows Operating System, must be versions currently supported by Microsoft, home versions are not allowed
	+ RAM 4GB minimum
* Warranty
	+ *Workstations and laptops should carry a current warranty*
* Security
	+ Remote Monitoring agent installed and functioning properly
	+ Supported Antivirus installed and functional; all other AV products removed; device is infection free
	+ *Wake on LAN capable and configured*
	+ User Access Control will be enabled on workstations for Domain Users
* Continuity
	+ To the extent it is possible, data should be stored on servers through the use of mapped drives.
	+ Data that cannot be stored centrally should be backed up by the file-level Cloud backup service – for example laptops that are frequently off the network.
	+ System Restore will be enabled for all workstations.
* Network Setup
	+ *DHCP*
	+ *Wired connection recommended*
* Printers configured through GPO and printing through print server
	+ All printers must be connected to the network via Ethernet or wireless
	+ Printer must have a static IP address

# Additional Requirements Specific to Apple

* RAM minimum is 8GB if running Apple OS and Windows Virtual Machine
* Apple OS updates are current and configured to auto update
* OSX Recovery is enabled
* Windows Virtual Machine (If installed)
	+ Must use VMWare Fusion or Parallels (Most current version)
	+ Windows install must conform with [RMM Workstations](file://connect.greatamerica.com/DavWWWRoot/sites/collabrance/MSP/RunBook/Shared%20Documents/RMM%20Workstations.docx)
	+ AV may be installed only on the VM side under this setup

# Thin Clients

* Write Protection mode must be enabled
* Minimum 20GB flash memory
* Minimum 4GB RAM
* Thin clients must be joined to the domain
	+ Remote users must be joined to the domain over a site-to-site VPN tunnel or an MPLS circuit

# Applications

* Microsoft Office versions must be supported by Microsoft and have licensing information and the location of media/install files documented
* *All users should have the same version of MS Office*
* *Within a given subscriber, all Office installs should be licensed the same way*
* *LOB apps – need a current support contract*

# Onboarding Timeline

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Today** | **Contracts Signed *(Day 3)*** | **HW/SW Acquisition *(Day 4)*** | **Phase 1 *(Day 7)*** | **Go Live *(Day 14)*** | **30 Day Review *(Day 30)*** | **Phase 2 *(Driven by Warranty/Tech Plan)*** | **Q3 Business Review*****(Monthly/Quarterly)*** |
| **Stabilize** |   |   |   |   |   |   |   |   |
| **Standardize** |   |   |   |   |   |   |   |   |
| **Maintain** |   |   |   |   |   |   |   |   |
| **Optimize** |   |   |   |   |   |   |   |   |