M3Networks

MSP CLIENT HANDBOOK

HARNESSING THE FULL POWER OF YOUR IT NETWORK

Your Guide to Using and Getting Support for your Technology

TABLE OF CONTENTS

A NOTE FROM THE CEO

Hello and Welcome!

I wanted to personally thank you for joining our growing community of tech-savvy, forward thinking business owners! We are excited to start helping you implement state of the art IT solutions to power your enterprise.

As you'll come to learn, here at M3 Networks we are passionate about empowering each and every one of our clients with the best tools to grow, optimize and protect their businesses.

We love coming up with creative solutions to complex technical challenges and helping businesses increase their profitability and competitive edge by using the right tools to maximize efficiency and facilitate innovation.

This Client Handbook contains all the information you need to get the most out of your technology, along with our important policies that ensure that things are always on track and running smoothly.

Please take some time to familiarize yourself with the contents, sign all forms where indicated, and distribute copies of important policies to your team so we can provide you with fast, efficient and world-class support.

Again, we're excited to have you on board and looking forward to working with you!

Here to serve,

Michael Moore

WHAT CAN WE HELP WITH?

At M3 Networks, We're not just Computer People – We can also help you with various other business technology needs, including:

- ⇒ IT Consulting, including budgeting, business automation and strategic planning
- ⇒ Disaster recovery and business continuity planning
- ⇒ Domain name procurement, hosting, and renewals
- ⇒ Project planning and management

In addition, we have a network of **Trusted Partners and Advisors** for services such as Accounting, Legal, Marketing and more – so if You're looking for a referral, don't hesitate to get in touch with Us via your **Account Manager** to find out whether we can help you or point you in the right direction!

STANDARD TECHNOLOGY SUITE

There are countless options for small businesses looking to implement technology to support their operations. As IT professionals, it is our job to keep up with the developments in this rapidly evolving industry and ensure that our clients are using the best technology in terms of reliability, speed, security, integration, and fit for their business needs and objectives.

After many years of serving exclusively small and growing businesses, We have curated a list of technologies that work well together and enable us to create IT networks that suit the needs of any business – we call this Our **Standard Technology Suite** (or "**STS"**).

Below is the list of the technologies that We currently use to create a well-integrated, reliable and secure IT infrastructures for each of Our clients:

Hardware

- ✓ Dell Servers & Storage
- ✓ Dell Desktops & Laptops
- ✓ Canon, Samsung, Dell, or HP Printers
- ✓ Cisco Wireless Access Points
- ✓ SonicWall Routers & Firewalls
- ✓ Dell, Cisco, or Netgear Network Switch
- ✓ 8x8 Phone Systems

Software

- ✓ Microsoft 365
- ✓ Microsoft Azure
- ✓ Microsoft Windows 10 and Above
- ✓ Remote Access
- ✓ Anti-virus & Endpoint Detection and Response
- ✓ Managed Detection & Response with 24/7 US Based SOC
- ✓ Email SPAM Filter
- ✓ Email Backup
- ✓ Workstation Automation
- ✓ Workstation Back-up
- ✓ Password Manager
- ✓ DNS Security

- ✓ Server Back-up (if applicable)
- ✓ Security Awareness Training
- ✓ Phishing Simulation
- ✓ Dark Web Monitoring
- ✓ Office 356 Monitoring

We continue to educate Ourselves and train Our teams on the most up-to-date information on each component in Our STS, so that Our clients never miss out on the latest updates and developments such as new software solutions, upgraded functionality, and cybersecurity protections. Because the field of technology is constantly evolving, We often amend the list of hardware and software We use to provide you with the best IT infrastructure and the best security solutions to protect against the ever evolving cybersecurity risks threatening small businesses.

While We are smart enough to troubleshoot almost any issue with any product, and We can most likely work with any hardware and software that are not listed above, any tasks involving the installation, setup, maintenance and support of those products is outside of the scope of any Managed Service Plan, and is billed hourly, at the rates outlined in Your Master Service Agreement.

HOW CAN I GET FAST SUPPORT?

All Service Requests must be initiated by one of the methods outlined below. When requesting a service, You must provide a detailed description of the issue and the specific services requested.

	**USE THE WEB PORTAL** This is the fastest and easiest way to get help. Simply log into your account at https://portal.m3networks.com/ Select "Support" from the drop down menu at the top, then click "Submit a Support Ticket". Just follow the steps, provide all the requested information, and hit "Submit" at the end of the form.
	**SEND US AN EMAIL** If you prefer not to use the website, you may always shoot us an email to support@m3networks.com to open a ticket as well. Please include a brief summary of your issue in the subject line, and provide a detailed description of the issue in the body of the email. Once you hit send, look for the automated reply to confirm that your request was received.
	**CALL US** You can call us **M-F 8am-5pm CST** at **817-532-0127** whenever you need help.

If you have an EMERGENCY or require after-hours support, you MUST either call us and mention the issue is an Urgent Request or email us at support@m3networks.com with Urgent Request as the Subject of the Email.

RESPONSE TIMES

IMPORTANT NOTE

If you send emails to our **Direct Email Addresses** or call us on our **Cell Phones**, this will result in slower response times. Using the above methods to contact us is the only way to ensure a quick and reliable response within our **Guaranteed Response Time Frames**.

In order to ensure that the most pressing issues are responded to the quickest, We categorize and respond to each service request based on the severity/urgency (or "Priority") of the issue. This means that when we get a service request on an issue we deem Critical, we start working on it within an hour, while lower priority tasks will be responded to a bit slower (but still within the guaranteed response times).

Determining the priority of an issue is within Our sole discretion; however, to give an idea of what to expect, priorities are generally assigned as shown in the table below. Our Priority classifications correspond to Our Guaranteed Response Times (column 3), so that the highest priority issues are responded to in the quickest time frame.

PRIORITY	ISSUE / IMPACT	EXAMPLES	GUARANTEED RESPONSE TIMES*	TARGET RESOLUTION TIMES**
Urgent	**Service not available (all users and functions unavailable)**. Entire office is shut down, unable to work, or experiencing severe inconvenience. Significant cybersecurity risk.	Your Main Server is offline/inaccessible and all users are unable to work.	**1 Hour**	**1-4 Hours**
		One of your Network Switches has failed or a VPN link is offline and half the users cannot work.		
		Internet service is down		
		Complete hardware failure		
		Ransomware attack or other serious cybersecurity breach		
High	**Significant degradation of service (large number of users or critical functions affected)**. Major workflow impact for one or more users.	There is a suspected virus on a machine	**2 Hours**	**2-8 Hours**
		Your CEO's computer has stopped working and they have an urgent task		
		Your main payroll, accounting or other critical software has stopped working		
		Central printing not working		
	Limited degradation of service. Limited	A single user's computer is not working	**4 Hours**	**48 Hours**

Medium	number of users or functions affected, business process can continue.	A user's printer is not working, but they can print to another machine		
		Single user wireless connectivity issues, slow computers, software updates for the whole network or multiple users		
Low	**Small service degradation (business process can continue, one user affected)**. Requests relating to future planning; very low-impact requests; desired upgrades and improvements.	Printing is slower than normal	**8 Hours**	**5 Days**
		A new employee needs user access setup		
		A user needs a software update or new software installed		
		Planning network changes and improvements for future plans/growth		

All issues must meet the above guidelines for each priority level to be classified as such. For instance, if multiple users are having connectivity problems, that would be considered a High Priority ticket. If it is submitted as an Urgent request, we reserve the right to reassign it to High Priority and take care of any Urgent tickets in queue first. Similarly, if a desktop printer malfunction is submitted as a High Priority ticket, we will reassign it as a Medium Priority ticket and handle any higher priority issues first.

All examples above are provided solely as an illustration of the types of issues that fall under each priority level, and should only be used to gain an understanding of how we rank urgency, rather than an exhaustive list of issues under each priority.

HOW DO I ESCALATE AN ISSUE?

If You wish to move a Service Request up to a higher priority than it would normally be assigned pursuant to the table above (for example, requesting that a printer malfunction be treated as an Urgent Priority ticket), You may request a higher priority by:

- contacting Your Designated IT Contact
- Submitting a request for escalation of an existing Service Request at https://portal.m3networks.com/
- contacting Us at email/phone

When You do any of the foregoing, We will treat Your Service Request as a Critical Priority Issue. Please note that all labor performed on services classified as Emergency Upgrades are billed at our emergency rate.

Additionally, if you ever feel that we're not handling your request as well as we could be, you can escalate that issue by giving Us a call at 817-532-0127 or sending an email to support@m3networks.com.

Our team is highly capable, efficient and professional, we do hope that you'll never need to use this process; however, in the unlikely event that we make a mistake or our response doesn't meet your expectations, you can count on us to own up to it and fix the issue ASAP!

AFTER HOURS AND EMERGENCY SUPPORT FORM

Would you like to implement restrictions on after hour support request?

- ☐ Yes – continue filling out the rest of the form
- ☐ No- Sign bottom of the page

Staff/Management who can approve after hour request: If you would like a specific member of your staff or management to approve all emergency upgrades and after-hours requests, please list the best way to contact that person after hours. If you are listing multiple personnel, please list them in order of whom you would like for us to reach out to first. If you have different approvers per location, please use the location field.

Name	Phone Number	Location

If we are unable to reach management for approval, please document here how you would like for us to proceed:

_____
_____
_____

Any other restrictions or approval process request:

_____
_____
_____

SUPPORT TIERS

The following table describes our Support Tier levels and how issues are moved between tiers to ensure that each issue is handled by the appropriate technician:

SUPPORT TIER	DESCRIPTION
Tier 1 Support	All support incidents begin in **Tier 1**, where the initial trouble ticket is created, and the issue is identified and clearly documented, and basic hardware/software troubleshooting is initiated.
Tier 2 Support	All support incidents that cannot be resolved with Tier 1 Support are escalated to **Tier 2**, where more complex support on hardware/software issues can be provided by more experienced Engineers.
Tier 3 Support	Support Incidents that cannot be resolved by Tier 2 Support are escalated to **Tier 3**, where support is provided by the most qualified and experienced Engineers who have the ability to collaborate with 3rd Party (Vendor) Support Engineers to resolve the most complex issues.

LETTER TO VENDORS FOR AUTHORIZATION

Sometimes vendors require written authorization from You before they can discuss matters related to your business with Us. To help with obtaining such authorization, feel free to copy and paste this text on to your letterhead or into your email, and modify it to suit each vendor that We will need to work with while performing the Services.

EMAIL SCRIPT

To Whom It May Concern,

This letter is to inform you that we have contracted M3 Networks to manage our IT and Technology needs.

To be able to do this effectively, M3 Networks needs to be able to support and manage all of our technology suppliers on our behalf.

As such, this letter authorizes anyone from the team at M3 Networks to access and modify all aspects of our account and all the products and services that we have with effective immediately.

This authorization is valid until we give you written notice otherwise.
Should you require any further details, please let us know.

Regards,

CONTACTS & COMMUNICATIONS

YOUR DESIGNATED IT CONTACT(S)

As part of your Onboarding, we asked you to appoint one or more **Designated IT Contacts** from your business. Designated IT Contacts must be:

- ⇒ the person responsible for submitting Service Requests on behalf of Your organization, an office location or for an internal department or team;
- ⇒ authorized to request and make changes to Your IT Network and any associated account(s), including but not limited to adding or deleting users, deleting data, changing or terminating subscriptions and other Services, and ordering hardware/software;
- ⇒ the person whom We can contact in case We need more information about an issue or if We need to send important information about an issue We are working on.

This is a security policy that is in place for Your protection, as we do not want to expose any confidential data to any user who does not have authority to access same, or to bind your organization to user agreements and/or make changes to your account or IT network on the instruction of personnel who are not authorized to make such decisions.

YOUR ACCOUNT MANAGER

During Onboarding You will be assigned an Account Manager who will be responsible for understanding Your business model, operations and objectives, and ensuring that in light of all of these factors, Your IT Network truly meet the needs of your organization at every stage.

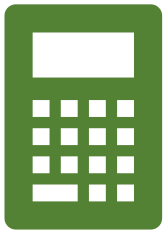
Your Account Manager is the point of contact for all discussions relating to Your business as a whole, any upcoming projects, changes in Your operations, future plans,

IMPORTANT NOTE

Your Account Manager is not part of the Helpdesk Support Team. Never contact your **Account Manager** for Service Requests, which should always be submitted using the methods outlined in this Handbook to avoid delays!

budgeting, and other high-level issues, questions or concerns. Your Account Manager is also the team member that will be conducting your Quarterly Reviews.

ACCOUNTING & BILLING CONTACT



Should you have any billing or accounting questions, simply send us an email to account@m3networks.com and someone in our accounting department will be in touch.

You can also call Us during regular business hours at 817-532-0127 or log into your account https://portal.m3networks.com/ to view your billing history and download copies of past invoices and other documents.

SECURITY POLICIES

As you probably know, every minute of every day, millions of computer networks experience security breaches that result in business interruption, data loss, and money damages. Ransomware attacks are on the rise, as well as misappropriation of personal and proprietary information from computer networks that result in end-user damages (such as account breaches, fraudulent purchases using stolen financial information, and identity theft), which in turn leads to lawsuits, claims and government fines levied against the business whose network the information was obtained from.

Hackers and other criminals actively target companies, because they know businesses have a lot to lose in the form of capital, clientele, and possible fines for inadequate security. They also know that as a result, businesses will more often than not find a way to come up with the money to pay any ransom to regain access to the data and networks they need to continue operations.

Due to the severity of this ongoing threat, it is important for Us to ensure that Your systems are as secure as possible – while at the same time keeping the network usable and efficient.

Though We do implement as many state-of-the-art cybersecurity solutions to run in the background as possible with the budgets You provide Us to work with, We also supplement these protections with policies for Your team to follow, which are designed to increase Your defense against the most common threats and attacks.

All of Our important security policies are contained in the IT Policy Manual, so they are easy to keep track of and reference when needed. Please take the time to read through this Manual, and ensure that all team leaders responsible for compliance and the drafting/implementation of internal policies attend all of Our Scheduled Security Trainings, where We go through each Policy in detail and answer any questions You may have.

Additionally, We are always available to explain and help You implement the Security Policies in Your business.

HANDBOOK ACKNOWLEDGEMENT

I acknowledge that I have received and read the Client Handbook, and that I understand and agree to follow the requirements set forth above, and as may be supplemented or modified via amendment from time to time.

I further acknowledge and agree that failure to follow the requirements and processes set forth in the Client Handbook absolves M3 Networks from any liability whatsoever in connection with any delays, losses or damages which may occur as a result.

_____

_____
Date