



Good People, Great IT!

CLIENT HANDBOOK

**HARNESSING THE FULL POWER
OF YOUR IT NETWORK**

Your Guide to Using and Getting Support for your Technology

A NOTE FROM THE CEO

Hello and Welcome to the JPtheGeek Family!

I want to personally thank you for trusting JPtheGeek with your IT and cybersecurity needs. We're excited to be your partner in ensuring that your technology works seamlessly, securely, and in a way that helps your business grow.

At JPtheGeek, we don't just fix IT issues—we proactively manage, protect, and optimize your technology so you can focus on what matters most: running your business. Our team of geeks is passionate about problem-solving, innovation, and building strong relationships with our clients. We believe that IT should be a strategic advantage, not a headache, and we're here to make sure it works for you, not against you.

This Client Handbook is designed to help you get the most out of your partnership with us. Inside, you'll find important information about our services, how to request support, our response times, security policies, and more. Our goal is to keep things simple and transparent so you always know what to expect.

Please take a moment to review the contents, sign any required forms, and share relevant policies with your team. This will ensure that we can provide you with the fastest, most efficient, and highest level of service possible.

We're thrilled to have you on board and look forward to supporting your success! If you ever have questions, need help, or just want to geek out about tech, we're just a call or message away.

Welcome to the JPtheGeek family!

Best Regards,
Jesse Pearson
Founder & CEO, JPtheGeek

WHAT CAN WE HELP WITH?

In addition to managing and protecting your IT Network, we can also help you with various other business technology needs, including:

- ⇒ AI Consulting & Implementation
- ⇒ Conference Audio and Video planning, procurement and installation
- ⇒ IT Consulting, including budgeting, business automation and strategic planning
- ⇒ Disaster recovery and business continuity planning
- ⇒ Domain name procurement, hosting, and renewals
- ⇒ Cloud Hosted Voice
- ⇒ Cloud Hosted Fax
- ⇒ Security Cameras
- ⇒ Access Control
- ⇒ Burglar Alarm Systems
- ⇒ Low Voltage Cabling
- ⇒ Project planning and management

STANDARD TECHNOLOGY SUITE

There are countless options for small businesses looking to implement technology to support and enhance 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

- ✓ HP, Dell, or Lenovo Servers & Storage
- ✓ Lenovo or HP Desktops & Laptops
- ✓ HP Enterprise Printers (through our partner)
- ✓ Meraki or Ubiquiti Network Equipment
- ✓ Meraki, Sophos, Fortinet, and SASE Routers & Firewalls
- ✓ Currently supported IP Phones

Software

- ✓ Microsoft 365
- ✓ Microsoft Azure
- ✓ Cloud Hosted Phone Systems
- ✓ Supported versions of Microsoft Office

- ✓ Supported versions of Microsoft Windows
- ✓ Supported versions MacOS, IOS, iPadOS
- ✓ Supported versions of Android

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. Any time we make a change to our STS, we will post the new version to <https://ipthegeek.com/handbook-policies/>

While we are able to troubleshoot almost any issue with any product, and can likely work with a large selection of hardware and software 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 thus billed hourly, at the rates outlined in your Master Service Agreement.

HOW CAN I GET 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.

1. USE THE WEB PORTAL

This is the fastest and easiest way to get help. Simply log into your account at <https://support.ipthegeek.com>. From here you can submit forms for standard support issues, new employees, departing employees, etc.

2. SEND US AN EMAIL

If you prefer not to use the website, you may always shoot us an email to support@ipthegeek.com and provide a detailed description of the issue. After you send the email, look for the automated reply to confirm that your request was received.

3. CALL US

You can call us **M-F 8 am-5 pm EST** at **(317) 936-3300** whenever you need help.

If you have an EMERGENCY or require after-hours support, you **MUST** call us. Otherwise the issue will be responded to during regular business hours within the queue. If you submit a request that has any specific due dates or times or is urgent, you must specify this in your ticket or request.

IMPORTANT: 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 Response Time Frames.

RESPONSE TIMES (Service Level Objectives)

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.

Business Standard Package Clients

PRIORITY	ISSUE / IMPACT	EXAMPLES	GUARANTEED RESPONSE TIMES*	TARGET RESOLUTION TIMES**
Urgent	Service not available (all or majority of users and functions unavailable). Entire office is shut down, unable to work, or experiencing severe inconvenience. Significant cybersecurity risk.	Your main server is inaccessible.	1.5 Hours	1-4 Hours
		A VPN link is offline and the majority of users cannot work		
		Internet service is down		
		Complete hardware failure or failure of a key software affecting the majority of users		
		Ransomware attack or other serious cybersecurity breach		
High	Significant interruption 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
		Key personnel’s computer has stopped working and they have an urgent task		
		Your main email, payroll, accounting or other software critical to operations has stopped working		
		Central printing not working		
Medium	Moderate interruption of service. Limited number of users or functions affected, business process can continue.	A single user’s computer is not working	4 Hours	48 Hours
		A single printer is not working, but other machines are available		

		Single user wireless connectivity issues, slow computers, software updates		
Low	Minor service interruption (business process can continue, one user affected). Requests relating to future planning; very low-impact requests; desired upgrades and improvements.	Internet, printing and other functions are slower than usual, but still working	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		
No Priority	All email received tickets come in at this priority. If there is no priority requested within the ticket from the user, and our team cannot easily and quickly determine if this is an urgent request. It will remain here or at Low priority.	All other requests that do not necessarily fit into another category, or cannot be quickly and easily determined by our team.	None	None

Business Critical Package Clients

PRIORITY	ISSUE / IMPACT	EXAMPLES	GUARANTEED RESPONSE TIMES*	TARGET RESOLUTION TIMES**
Urgent	Service not available (all or majority of users and functions unavailable). Entire office is shut down, unable to work, or experiencing severe inconvenience. Significant cybersecurity risk.	Your main server is inaccessible.	30 Minutes	1-4 Hours
		A VPN link is offline and the majority of users cannot work		
		Internet service is down		
		Complete hardware failure or failure of a key software affecting the majority of users		
		Ransomware attack or other serious cybersecurity breach		
High	Significant interruption of service (large number of users or critical functions affected).	There is a suspected virus on a machine	1 Hour	2-8 Hours
		Key personnel's computer has stopped working and they have an urgent task		

	Major workflow impact for one or more users.	Your main email, payroll, accounting or other software critical to operations has stopped working		
		Central printing not working		
Medium	Moderate interruption of service. Limited number of users or functions affected, business process can continue.	A single user's computer is not working	4 Hours	48 Hours
		A single printer is not working, but other machines are available		
		Single user wireless connectivity issues, slow computers, software updates		
Low	Minor service interruption (business process can continue, one user affected). Requests relating to future planning; very low-impact requests; desired upgrades and improvements.	Internet, printing and other functions are slower than usual, but still working	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		
No Priority	All email received tickets come in at this priority. If there is no priority requested within the ticket from the user, and our team cannot easily and quickly determine if this is an urgent request. It will remain here or at Low priority.	All other requests that do not necessarily fit into another category, or cannot be quickly and easily determined by our team.	None	None

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.

Our Response Time Guarantee. Unless a service is excluded from our Guaranteed Response Times, we will respond to your Service Requests within the Guaranteed Response Times outlined above. **“Respond”**

in this context means that we will assign a technician and begin working on the issue within the applicable time frames, and should not be confused with *resolving* the issue, which is often unpredictable and subject to many factors outside of our knowledge and control until we actually begin work on the problem. We reserve the right to amend this list by providing you a revised set of Guaranteed Response Times via an amended Client Handbook or other similar policy document issued by Us.

Our Response Time Guarantee does not apply to Service Requests lodged outside of Business Hours.

Target Resolution times are simply an objective and not guaranteed in any way. Many factors are outside of our control in the time it takes to resolve an issue therefore we cannot guarantee any time frames on resolution.

We are serious about our guarantees and want to do what we can do make it right should we fail to abide by them for any reason. If you reported an incident to us via the appropriate channels and Our response time exceeds the Guaranteed Response Time for that issue, You may make a claim for credit within 7 days of the incident in writing to accounts@ipthegEEK.com. If we agree that Your claim is valid, You will be credited \$50 towards your next monthly bill per occurrence.

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 an “Emergency Upgrade” by:

- Calling the office at (317) 936-3300

When You do, We will treat Your Service Request as a Critical Priority Issue. Please note that all Labor performed on services classified as Emergency Upgrades could be billed at our emergency rate of \$350 per hour, minimum of two hours if they do not fall within our standard emergency triage process.

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 (317) 936-3300 or sending an email to accounts@ipthegEEK.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

If you would like to make restrictions as to who can request after hours support please contact your account manager at accounts@ipthegEEK.com to notify them of which users who can utilize after hours support. If you want to limit this, please send us a list using the template (table and fields) below to let us know who can use/approve after hours/emergency support.

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	All support requests begin in Tier 1 , where the ticket or work order is created, the issue is identified and documented, and basic troubleshooting measures are initiated.
Tier 2	All service requests that cannot be resolved at the Tier 1 level are moved to Tier 2 , where more complex support can be provided by more experienced Engineers.
Tier 3	Issues that cannot be resolved by Tier 2 engineers are escalated to Tier 3 , our most qualified and experienced Engineers. These personnel have the highest skill level and the

	ability to collaborate with 3 rd Party (vendor) support to resolve difficult issues.
--	-------------------------------------------------------------------------------------------------

VENDOR AUTHORIZATION LETTER

Sometimes vendors require written authorization from you before they can discuss matters related to your business with us. To help obtain such authorization, feel free to customize and copy the letter below into an email to each vendor that needs authorization to work with us while we provide our services:

Dear <Vendor Name>,

I am writing to notify you that we have engaged JPtheGeek LLC to oversee and handle our IT and Technology requirements.

In order to execute these responsibilities, it is essential that JPtheGeek LLC has the authority to coordinate, manage and obtain support as needed from all of our technological vendors and resources.

Therefore, effective immediately, we grant full permission to any member of the team at JPtheGeek LLC to access, modify, and manage all facets of our account, including all products and services we have obtained through your organization.

This authorization will remain in effect until we formally rescind it in writing. If additional information is needed, please do not hesitate to contact us.

Sincerely,

[Name]

[Title]

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

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!

ACCOUNTING & BILLING CONTACT

Should you have any billing or accounting questions, simply send us an email to billing@ipthegeek.com and someone in our accounting department will be in touch. You can also call us during regular business hours at (317) 936-3300 or log into your account at <https://ipthegeek.connectboosterportal.com/platform/login> to view your billing history and download copies of past invoices and other documents.

COMMUNICATIONS STANDARDS

Communicating With Us. In order to create a high-quality working relationship, You agree to:

- communicate with Us honestly, timely, and with clarity/specificity regarding what is needed (including timely responding to Our communications and timely reporting any issues or problems so that We can address them before they lead to greater issues);
- refrain from sending excessive emails, messages, phone calls and voicemails, and from multiple follow-ups before the reasonable response times stated in this Handbook has expired;
- remain open to feedback and assistance;
- be available to participate fully in meetings and calls, online and on-site; and

- give Us feedback about any issues or desired changes, so that We can make improvements and render the most effective assistance possible.

Prohibited Conduct. The following conduct is prohibited, constitutes a material violation of Your Master Service Agreement, and may result in the immediate termination of Our services to You:

- any bullying, disrespectful or disruptive behavior of any kind, including the use of profanity, insulting, or raising Your voice when speaking to any of Our team members, vendors, affiliates or clients;
- engaging in any conduct that violates any law, statute, ordinance or regulation;
- engaging in communication, making any statement, or posting/sharing any content or information that:
 - is malicious, inaccurate, unfounded, or slandering information that serves the purpose of defaming or discrediting Us or any of Our team members, employees, affiliates or agents;
 - causes harm, damage, injury or the violation of the rights of any person or entity under the law;
 - known or is reasonably foreseeable to cause harm or damage to minors;
 - is hateful, defamatory, bullying, obscene, racially or religiously offensive, abusive, harassing, or threatening.

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 defence 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. We will work with you during your onboarding to draft/implement these for your organization.

Additionally, we are always available to explain and help you implement the Security Policies in your business.