

Pegasys Technologies

Managed Services Terms and Conditions

Table of Contents

Table of Contents.....	1
1. Purpose and Structure.....	3
2. Order of Precedence.....	3
3. Scope of Services.....	3
4. Support Model.....	3
4.1 Service Desk.....	3
4.2 Incident Management.....	3
4.3 Service Requests.....	3
4.4 Escalation.....	3
4.5 Monitoring.....	3
5. Coverage and Availability.....	3
6. Schedule A: Service Offering.....	4
7. Client Responsibilities.....	4
7.1 Access and Cooperation.....	4
7.2 Supported Systems.....	5
7.3 Security Responsibilities.....	5
7.4 Backup and Data Responsibility.....	5
7.5 Required Client Contacts.....	5
8. Change Management.....	5
9. Schedule B: Excluded Services.....	5
9.1 Project Work.....	5
9.2 Third-Party Costs.....	6
9.3 Unsupported or Non-Standard Systems.....	6
9.4 Client-Caused or Third-Party-Caused Issues.....	6
9.5 Personal or Non-Business Support.....	6
10. Fees, Billing, and Payment Terms.....	6
11. Microsoft 365, Cloud, and Subscription Licensing.....	7
12. Product Sales, Hardware, and Software.....	7

13. Professional Conduct and Mutual Respect	8
13.1 Unacceptable Conduct	8
13.2 Pegasys Rights Related to Conduct Issues	8
14. Confidentiality	8
15. Data Protection and Information Security	8
16. Warranty Disclaimer	9
17. Limitation of Liability	9
18. Indemnification	9
19. Term, Renewal, and Termination	9
20. Acceptable Use	9
21. Insurance	10
22. Non-Solicitation	10
23. Dispute Resolution	10
24. Force Majeure	10
25. General Terms	10
Appendix B: Acceptance and Signature	10
Attorney Review Checklist	11

These Managed Services Terms and Conditions establish the standard legal, operational, billing, and service framework under which Pegasys Technologies provides managed information technology services to its clients.

This Agreement is incorporated into and made part of any signed Quote, Statement of Work, Order Form, Managed Services Proposal, Service Agreement, or other written service document between Pegasys Technologies and the Client.

Together, these documents form the complete agreement between the parties.

1. Purpose and Structure

These Managed Services Terms and Conditions establish the standard legal, operational, billing, and service framework under which Pegasys Technologies provides managed information technology services to its clients. This Agreement is incorporated into and made part of any signed Quote, Statement of Work, Order Form, Managed Services Proposal, Service Agreement, or other written service document between Pegasys Technologies and the Client. Together, these documents form the complete agreement between the parties.

2. Order of Precedence

If there is a conflict between documents, the following order will apply:

1. Signed Statement of Work, Quote, Order Form, or Service Proposal
2. These Managed Services Terms and Conditions
3. Schedules, appendices, service descriptions, or supporting documents
4. Any Client purchase order or internal vendor document, only if specifically accepted in writing by Pegasys Technologies

Any preprinted or standard terms included in a Client purchase order, vendor onboarding form, procurement document, or similar document will not modify this Agreement unless expressly accepted in writing by Pegasys Technologies.

3. Scope of Services

Pegasys Technologies provides outsourced and co-managed IT services, which may include support, monitoring, maintenance, cybersecurity tools, cloud administration, backup monitoring, vendor coordination, project services, and advisory services as defined in the applicable SOW or Quote.

Services are limited to the systems, users, devices, locations, tools, and service categories specifically included in the applicable SOW, Quote, or Service Proposal.

Any service, system, location, device, application, user, project, or request not specifically included is considered out of scope and may be billed separately.

4. Support Model

Pegasys uses a structured service model to manage support requests, incidents, service requests, alerts, and changes.

4.1 Service Desk

The Service Desk is the primary point of contact for support requests, service issues, user assistance, troubleshooting, and ticket communication.

4.2 Incident Management

Pegasys will use commercially reasonable efforts to restore normal service operation as quickly as practical when an unplanned interruption or service issue occurs.

4.3 Service Requests

Routine user requests, access changes, workstation questions, software assistance, and administrative IT requests will be handled through normal ticketing procedures.

4.4 Escalation

Issues may be escalated based on impact, urgency, technical complexity, vendor involvement, or management review.

4.5 Monitoring

Where monitoring tools are included, Pegasys may monitor covered systems for alerts, outages, performance issues, or security events. Monitoring does not guarantee that all issues will be detected before they impact the Client.

5. Coverage and Availability

Unless otherwise stated in the applicable SOW or Quote:

- Standard business hours are Monday through Friday, 8:00 a.m. to 5:00 p.m., excluding federal holidays.
- Monitoring may operate 24x7x365 where included.
- After-hours, emergency, weekend, or holiday support is not included unless specifically stated.
- After-hours work may be billed at Pegasys' then-current after-hours or emergency rate.
- Third-party vendor outages, carrier issues, cloud platform issues, software failures, and licensing interruptions are subject to the applicable vendor's availability and support terms.

6. Schedule A: Service Offering

Specific services will be defined in the applicable SOW or Quote. Standard managed service categories may include:

Service Category	Typical Scope
Managed Endpoint and Server Services	Workstation and server support; monitoring and alerting; patch management; endpoint protection support; performance and health monitoring; basic troubleshooting; user administration.
Cybersecurity Services	Endpoint detection and response; email security support; DNS filtering or web protection if included; identity and access support; security awareness tools if included; risk reduction guidance.

Cloud and Platform Management	Microsoft 365 user and license administration; cloud platform support; tenant configuration support; Mobile Device Management; permission and access support; vendor coordination.
Backup and Disaster Recovery	Backup configuration support if included; backup monitoring if included; alert review; restoration assistance where valid backups exist; disaster recovery planning if included.
Network Management	Firewall, switch, and wireless support if included; connectivity troubleshooting; network device coordination; ISP and vendor support coordination.
Help Desk Support	Remote support; onsite support if included; ticket lifecycle management; end-user troubleshooting; escalation coordination.
Advisory Services	Technology planning; budget guidance; roadmap recommendations; business reviews if included; operational and security recommendations.

7. Client Responsibilities

7.1 Access and Cooperation

The Client will provide timely access to systems, facilities, applications, vendor accounts, licensing portals, administrative credentials, documentation, and personnel reasonably required for Pegasys to perform the Services. The Client will ensure that Pegasys has any required permissions, consents, licenses, vendor approvals, or administrative access necessary to support the Client environment.

7.2 Supported Systems

The Client is responsible for maintaining supported hardware, supported operating systems, active warranties where appropriate, properly licensed software, business-grade internet connectivity, and supported security tools. If the Client uses unsupported, end-of-life, improperly licensed, misconfigured, or non-standard systems, Pegasys may limit support, bill remediation separately, or require upgrades before continuing support.

7.3 Security Responsibilities

Security is a shared responsibility. Pegasys may recommend, configure, monitor, or support security tools, but no provider can guarantee that systems will be free from compromise, interruption, unauthorized access, or data loss.

- Follow reasonable security recommendations
- Keep required security tools active
- Not disable monitoring, antivirus, EDR, backup tools, MFA, or other protection systems without Pegasys approval
- Notify Pegasys of suspected security incidents promptly
- Use properly licensed software
- Maintain reasonable internal access controls
- Ensure users follow safe technology practices

7.4 Backup and Data Responsibility

Where backup services are included, Pegasys will use commercially reasonable efforts to configure, monitor, and support backup systems as defined in the applicable SOW. Successful recovery depends on backup availability, configuration, retention, vendor performance, data integrity, and the Client's compliance with recommended backup practices.

7.5 Required Client Contacts

The Client will designate the necessary contacts and Pegasys may rely on instructions, approvals, and information provided by designated Client contacts.

- Authorized Decision Maker
- Primary Contact
- Technical Contact
- Billing Contact
- Security Contact
- Change Approver

8. Change Management

Changes to systems, services, users, devices, locations, licensing, security configurations, network infrastructure, or business applications must follow Pegasys' change process.

5. Request submission
6. Scope and risk review
7. Approval
8. Scheduling
9. Implementation
10. Validation
11. Documentation

Changes affecting pricing, service levels, risk, security, timeline, or scope require a written change order, updated SOW, or approved Quote. No out-of-scope work is included unless approved in writing.

9. Schedule B: Excluded Services

Unless specifically included in the applicable SOW or Quote, the following are excluded and may be billed separately.

9.1 Project Work

- Migrations
- New system deployments
- Server replacements
- Cloud migrations
- Major software upgrades
- Infrastructure builds
- New location setups
- Network redesigns
- Security remediation projects
- Compliance projects
- Large-scale onboarding or offboarding projects

9.2 Third-Party Costs

- Hardware
- Software
- Licensing
- Cloud consumption
- Vendor subscriptions
- Telecommunications charges
- Shipping, freight, taxes, and surcharges
- Manufacturer support
- Warranty renewals

9.3 Unsupported or Non-Standard Systems

- End-of-life hardware or software
- Unlicensed software

- Consumer-grade equipment
- Unsupported operating systems
- Systems modified by unauthorized third parties
- Environments that do not meet Pegasys minimum standards

9.4 Client-Caused or Third-Party-Caused Issues

- Unauthorized changes
- User-installed software
- Malware caused by unsafe user action
- Failed vendor updates
- Client-directed configuration changes
- Power, cabling, ISP, or environmental issues
- Support required due to noncompliance with Pegasys recommendations

9.5 Personal or Non-Business Support

- Personal devices unless specifically included
- Home networks unless specifically included
- Personal email, personal accounts, or personal software
- Non-business technology

10. Fees, Billing, and Payment Terms

Charge Type	Billing Timing	Payment Term
Recurring managed services	Billed monthly in advance	Net 15 unless otherwise stated
Hourly work	Billed as incurred or monthly in arrears	Due upon receipt
Project work	Billed by deposit, milestone, or completion as defined in the Quote or SOW	Due upon receipt unless stated otherwise
Hardware, software, subscriptions, licensing, and third-party charges	May require prepayment before purchase or activation	Due upon receipt
After-hours or emergency support	Billed at Pegasys then-current after-hours or emergency rate	Due upon receipt

Pegasys may require clients to maintain an active electronic payment method or auto-pay arrangement for recurring managed services. Exceptions may be approved by Pegasys in writing.

Invoices not paid when due may result in account review, payment reminders, service suspension warning, suspension of non-critical services, suspension of all services, or termination in accordance with this Agreement.

Pegasys may charge late fees or interest on past-due balances at the lesser of 1% per month or the maximum amount permitted by applicable law.

Payment Escalation Guide

Typical escalation may include: 0 to 5 days past due, payment reminder; 15 to 20 days past due, service suspension warning; 25 days past due for managed services, management review and suspension eligibility; 30 days past due for hourly, project, hardware, or software invoices, management review and suspension eligibility.

Service may remain suspended until all outstanding balances are paid in full or an approved written payment arrangement is in place. Pegasys is not responsible for service interruptions, data loss, licensing interruption, security risk, monitoring gaps, or operational impact resulting from suspension due to non-payment.

If Pegasys must use collections, legal action, arbitration, or other enforcement action to collect amounts owed, the Client agrees to pay all reasonable collection costs, court costs, arbitration costs, and reasonable attorneys' fees to the extent permitted by law.

The Client may not withhold payment, offset invoices, or delay payment based on unrelated disputes, service concerns, vendor issues, or pending credits unless agreed to in writing by Pegasys.

The Client is responsible for applicable taxes, shipping, freight, tariffs, environmental fees, vendor fees, licensing charges, cloud consumption, subscription costs, and third-party charges related to services or products provided under this Agreement.

11. Microsoft 365, Cloud, and Subscription Licensing

The Client is responsible for all software, cloud, and subscription licensing purchased or maintained on its behalf.

Certain licensing subscriptions, including Microsoft New Commerce Experience subscriptions, may be non-cancelable, non-refundable, or not reducible after the applicable vendor's cancellation window.

If Pegasys purchases or maintains licensing on behalf of the Client, the Client remains responsible for the full subscription commitment, even if the Client stops using the license, reduces users, moves to another provider, terminates services before the subscription term ends, or the vendor does not permit cancellation or reduction.

12. Product Sales, Hardware, and Software

Hardware, software, equipment, cloud services, and third-party products are provided subject to the applicable manufacturer, publisher, distributor, or vendor terms.

Pegasys does not provide warranties beyond those provided by the manufacturer or vendor.

Products may be non-returnable, subject to restocking fees, subject to vendor approval, or subject to cancellation restrictions.

Pegasys may require payment before ordering hardware, software, licensing, subscriptions, or third-party services.

Risk of delay, product availability, vendor backorder, shipping delay, manufacturer defect, or vendor support response belongs to the applicable vendor and is outside Pegasys control.

13. Professional Conduct and Mutual Respect

Pegasys Technologies is committed to maintaining a professional, respectful, and safe working environment for its employees, contractors, vendors, and clients. To support a productive business relationship, the Client agrees that its employees, contractors, representatives, vendors, guests, and end users will communicate and interact with Pegasys personnel in a professional and respectful manner.

Pegasys Technologies & The Client will:

- Treat personnel with courtesy and respect
- Communicate constructively during service issues, incidents, disputes, and escalations
- Follow established support, escalation, and communication procedures
- Provide accurate and complete information for service delivery
- Avoid abusive, threatening, discriminatory, harassing, intimidating, or offensive conduct

13.1 Unacceptable Conduct

- Verbal abuse, harassment, intimidation, or threats
- Discriminatory, hateful, or offensive language
- Repeated hostile or disruptive communication
- Personal attacks against personnel
- Client attempts to bypass service procedures through excessive escalation or unreasonable demands
- Knowingly providing false, misleading, or incomplete information
- Conduct that creates an unsafe, hostile, or unprofessional working environment

13.2 Pegasys Rights Related to Conduct Issues

- Request corrective action or written communication plan
- Require communication through designated contacts
- End a meeting, call, onsite visit, or written exchange
- Escalate concerns to Client leadership
- Terminate services if conduct continues or is severe

Pegasys will make reasonable efforts to resolve conduct concerns collaboratively. However, Pegasys is not required to subject its personnel to abusive, threatening, harassing, or unsafe conditions to provide services. The conduct described in this section is illustrative and not exhaustive.

14. Confidentiality

Each party may receive confidential, proprietary, technical, financial, operational, security, business, or client information from the other party.

Each party agrees to protect the other party's Confidential Information using reasonable care and to use such information only for purposes related to this Agreement.

Confidential Information does not include information that is publicly available through no fault of the receiving party, already known by the receiving party, independently developed without use of the disclosing party's information, lawfully received from a third party, or required to be disclosed by law, subpoena, court order, or government authority.

Pegasys templates, processes, documentation, security configurations, scripts, methods, reports, checklists, and technical procedures remain Pegasys confidential and proprietary information unless otherwise agreed in writing.

15. Data Protection and Information Security

Pegasys will use commercially reasonable safeguards designed to protect Client Data that Pegasys accesses, processes, or stores while providing services.

The Client understands that no security service, backup system, monitoring platform, cloud service, firewall, endpoint tool, or network configuration can guarantee absolute security, uninterrupted operation, or complete protection against unauthorized access, cyberattack, data loss, ransomware, vendor failure, or user error.

The Client remains responsible for its own business continuity planning, cyber insurance, employee training, access policies, internal controls, data classification, and regulatory obligations unless specifically included in a written SOW.

16. Warranty Disclaimer

Pegasys will perform services in a professional and commercially reasonable manner consistent with generally accepted industry standards.

Except as expressly stated in the applicable SOW, Pegasys does not warrant that services will be uninterrupted or error-free, all security threats will be detected or prevented, all data will be recoverable, all systems will be free from vulnerabilities, third-party services will remain available, vendor products will operate without failure, monitoring will detect every issue before impact, or recommendations will eliminate all risk.

17. Limitation of Liability

To the maximum extent permitted by applicable law, Pegasys will not be liable for indirect, incidental, special, consequential, exemplary, or punitive damages, including lost profits, lost revenue, loss of business opportunity, loss of goodwill, loss of data, business interruption, downtime, or third-party claims, even if Pegasys has been advised of the possibility of such damages.

Pegasys total cumulative liability for claims arising from or related to this Agreement, any SOW, or the Services will not exceed the fees paid by the Client to Pegasys for the affected Services during the six months immediately preceding the event giving rise to the claim.

18. Indemnification

Each party agrees to indemnify, defend, and hold harmless the other party from third-party claims, damages, liabilities, costs, and reasonable attorneys' fees arising from that party's material breach of this Agreement, gross negligence or willful misconduct, violation of applicable law, misuse of the Services, infringement of third-party intellectual property rights, failure to obtain required licenses or consents, or unauthorized or unlawful use of systems, software, data, or services.

The Client agrees to indemnify Pegasys for claims arising from Client content, Client data, Client systems, Client-provided software, Client instructions, Client users, or Client failure to follow required security, licensing, access, or compliance obligations.

19. Term, Renewal, and Termination

The initial term will be defined in the applicable SOW, Quote, Order Form, or Service Proposal. Unless otherwise stated, the Agreement will renew automatically for successive one-year terms unless either party provides written notice of non-renewal at least 60 days before the end of the then-current term.

If the Client terminates before the end of the committed term for any reason other than Pegasys uncured material breach, the Client remains responsible for fees due through the effective termination date, remaining committed monthly fees if stated in the SOW, non-cancelable vendor commitments, unpaid hardware/software/subscription/project fees, transition services, and collection costs where applicable.

Either party may terminate if the other party materially breaches this Agreement and fails to cure the breach within 30 days after written notice. Pegasys may terminate immediately or suspend services for non-payment, severe misconduct, unsafe working conditions, unlawful use, disabled security tools, licensing failure, or unreasonable legal, security, financial, or operational risk.

Upon termination, Pegasys will provide reasonable transition assistance on a time-and-materials basis, subject to payment of all outstanding amounts. Pegasys is not required to provide transition services, passwords, exports, documentation, licensing administration, or vendor coordination until all undisputed outstanding balances and required transition fees are paid, except where prohibited by law.

20. Acceptable Use

The Client and its users may not use Pegasys-supported systems or services for unlawful, abusive, fraudulent, or unauthorized purposes, including hacking, phishing, spamming, identity theft, financial fraud, malware distribution, unauthorized access, software piracy, harassment, illegal content, network attacks, or circumventing security controls.

Pegasys may investigate potential misuse and may suspend services, restrict access, require removal of offending content, or terminate services if misuse creates risk to Pegasys, the Client, another client, a vendor, or a third party.

21. Insurance

Each party is responsible for maintaining insurance appropriate for its business, which may include commercial general liability, workers compensation, professional liability, cyber liability, and property insurance.

The Client is solely responsible for insuring its own equipment, systems, data, business interruption risk, cyber risk, and personal property.

22. Non-Solicitation

During the term of this Agreement and for twelve months after termination, neither party will knowingly solicit for employment the other party's employees or contractors who were directly involved in providing or receiving services under this Agreement, unless otherwise agreed in writing.

This does not restrict general job postings, unsolicited applications, or hiring initiated independently by the employee without direct solicitation.

23. Dispute Resolution

The parties agree to attempt to resolve disputes first through good-faith management escalation.

If the dispute cannot be resolved through management escalation, the parties may pursue mediation, arbitration, or court action as stated in the applicable SOW or as otherwise agreed in writing.

Unless otherwise stated in the applicable SOW, this Agreement will be governed by the laws of the State of Washington, without regard to conflict-of-law principles. Venue for any legal action will be in the state or federal courts located in Washington, unless otherwise required by law.

24. Force Majeure

Neither party will be liable for delay or failure to perform, except payment obligations, caused by events beyond its reasonable control, including natural disasters, fire, flood, power failure, labor disruption, war, terrorism, civil unrest, government action, internet outage, vendor outage, supply chain disruption, epidemic, pandemic, or failure of third-party services.

25. General Terms

The parties are independent contractors. Nothing in this Agreement creates a partnership, joint venture, employment relationship, agency relationship, or fiduciary relationship.

Neither party may assign this Agreement without the other party's written consent, except in connection with a merger, acquisition, reorganization, or sale of substantially all assets.

This Agreement may only be modified in writing by authorized representatives of both parties.

If any part of this Agreement is found unenforceable, the remaining provisions will remain in effect.

Failure to enforce a provision does not waive the right to enforce that provision later.

This Agreement, together with the applicable SOW, Quote, Order Form, Service Proposal, schedules, and addenda, represents the complete agreement between the parties and replaces prior discussions or understandings about the same subject matter.

Appendix B: Acceptance and Signature

By signing, the parties acknowledge that they have read, understood, and agree to these Managed Services Terms and Conditions together with the applicable SOW, Quote, Order Form, or Service Proposal.