



Information Understructures

IU's *Managed Network Services* is a comprehensive collection of services that provides well-defined, relevant, proactive, and remedial support for your IT infrastructure. These services can be employed as a supplement or alternative to your in-house IT staff.

When you let **IU** provide these services, you enjoy the certainty of knowing that key service and maintenance is being performed in an efficient, economical, and accountable manner.

Your IT leadership staff can focus on utilizing the value of your IT system, rather than chasing problems, and “fitting in” maintenance now and then.

This document provides tables showing **IU's** service offerings for Physical and Virtual servers and workstations, as well as their single unit costs per month.

There are significant economies of scale when you retain **IU** to manage multiple servers and workstations. Therefore, **IU** provides significant discounts for multi-unit service.

All pricing is displayed in monthly service fee amounts per server or workstation. Clients with multiple servers under an agreement with us receive volume discounts as follows:

Server Count (Virtual or Physical)	Discount
1	0%
2-5	10%
6-10	20%
11-25	30%
Workstation Count (Virtual or Physical)	Discount
1-10	0%
11-25	10%
26-75	20%



MANAGED NETWORK SERVICES SERVER BUNDLES

Service Bundle→	Small Business Server Standard Bundle		Small Business Server Premium Bundle		Windows Server Core Roles ⁱ Bundle		Windows Server Extended Roles ⁱⁱ Bundle	
	P ⁱⁱⁱ	V ^{iv}	P	V	P	V	P	V
Service ID	MNS-B01P	MNS-B01V	MNS-B02P	MNS-B02V	MNS-B03P	MNS-B03V	MNS-B04P	MNS-B04V
Asset Management	●		●		●		●	
Backup Audit Service	●	●	●	●	●	●	●	●
Critical Resource Monitoring Service	●	●	●	●	●	●	●	●
Customer Configuration Record	●	●	●	●	●	●	●	●
Email Management Service ^v	●	●	●	●			●	●
Email Monitoring Service ^{vi}	●	●	●	●			●	●
Health and Status Monitoring Service	●	●	●	●	●	●	●	●
Filesystem Maintenance	●	●	●	●	●	●	●	●
ISA Management ^{vii}			●	●			●	●
Helpdesk Service	●	●	●	●	●	●	●	●
Malware Mgmt Service	●	●	●	●	●	●	●	●
Onsite Inspection Service	●		●		●		●	
Patch and Update Service	●	●	●	●	●	●	●	●
Remote Support Service	●	●	●	●	●	●	●	●
Repair Management Svc	●		●		●		●	
Security Management Svc	●	●	●	●	●	●	●	●
SQL Server Mgmt Svc ^{viii}			●	●			●	●
System Admin Report	●	●	●	●	●	●	●	●
Technical Reserve Time	●		●		●		●	
Monthly Service Fee	\$495	\$395	\$595	\$495	\$395	\$295	\$595	\$495



MANAGED NETWORK SERVICES WORKSTATION BUNDLES

Service Bundle→	Networked Workstation Bundle		Isolated Workstation Bundle		Networked Thin Client Bundle
	P	V	P	V	P
Service ID	MNS-B11P	MNS-B11V	MNS-B12P	MNS-B12V	MNS-B13P
Asset Management	•		•		•
Backup Audit Service	•	•	•	•	
Critical Resource Monitoring Service	•	•	•	•	
Customer Configuration Record	•	•	•	•	•
Health and Status Monitoring Service	•	•	•	•	
Filesystem Maintenance	•	•	•	•	
Helpdesk Service	•	•	•	•	•
Malware Mgmt Service	•	•	•	•	
Onsite Inspection Service	•		•		•
Patch and Update Service	•	•	•	•	•
Remote Support Service	•	•			
Repair Management Svc	•		•		•
Security Management Svc	•	•	•	•	
System Admin Report	•	•	•	•	
Technical Reserve Time	•		•		•
Monthly Service Fee	\$75	\$50	\$75	\$50	\$25



INDIVIDUAL SERVICE DESCRIPTIONS

ASSET MANAGEMENT SERVICE: Asset Management Service is service to track your IT assets. IU maintains a record of each piece of covered equipment or software. Included in this record are details relating to brand, model, serial number, service ID, supplying vendor, date placed in service, assigned user, location, warranty expiration date, service contract or extended warranty data, scheduled replacement date, retirement date, method of disposition at retirement, and value at procurement, all as reported to IU by client.

Why This Service Is Useful: This service is useful for tracking assets reportable under property tax returns, forming the IT component for business insurance, planning replacement procurements, identifying shrinkage, and as an input for your disaster recovery and capacity planning.

BACKUP AUDIT SERVICE: Backup Audit Service is service to review and audit your file backup activities. IU reviews and audits your backup activity for completeness and correctness when compared to your pre-established plan. IU reports unsuccessful or missing backups to you.

Why This Service Is Useful: Successful backups of data are a critical resource for recovering from file system corruption, system failures, and losses. Because it can be a long time between the need for accessing backups, organizations can lose the discipline to assure that backups are performed as intended. This service provides an additional resource to review the success and discipline of your backup processes.



CRITICAL SERVER RESOURCE MONITORING SERVICE: IU monitors critical server resources for exhaustion. IU monitors each covered physical or virtual server running under a Microsoft Server operating system for the following conditions:

- a. Excessive processor utilization (>90% for a minimum of 10 minutes);
- b. Minimum boot volume free disk space (< 2GB);
- c. Minimum data volume(s) free disk space (<10%);
- d. Excessive memory utilization (>80%);
- e. Other parameters at IU's discretion.

IU attempts to discover the cause of critical resource exhaustion and take remedial action. Remedial action may include:

- a. Modifying the settings or configuration of the affected equipment or software;
- b. Recommending investments in upgrades or supplemental or additional equipment or software;
- c. Recommending changes in your workload allocation or processes;
- d. In cases where no comprehensive remedy is available, providing guidance as to how you may minimize the occurrence and impact of critical resource exhaustion.

Why This Service Is Useful: Anomalies occurring in a server often become more severe with the passage of time. Unresolved anomalies can cause system failure. Critical server resource exhaustion is an important predictor of failure. Many servers attempt to maintain normal operations even when facing resource exhaustion so the problem can be difficult to spot until it causes system failure. This service provides proactive monitoring of your server's critical resources with the goal of trapping and remedying the anomaly before system failure occurs.

CUSTOMER CONFIGURATION RECORD: This service maintains configuration documentation for covered equipment, software, and users. The documentation includes configuration, deployment, and security information.

Why This Service Is Useful: The Customer Configuration Record is used to support disaster recovery and ongoing maintenance activity. All significant maintenance actions require consideration of the structure and organization of an IT system. The Customer Configuration Record is a resource that can help limit unintended consequences during maintenance activities and is an important tool during disaster recovery.



HEALTH AND STATUS MONITORING SERVICE: IU monitors and measures the health, status, and performance of your equipment. Monitoring includes:

- a. Critical Events reported in the Event Log;
- b. Error logs and other logs related to performance;
- c. Event communications initiated by the Covered Equipment or Software;

IU attempts to discover the cause of the adverse events described above and takes remedial action. Remedial action may include:

- a. Modifying the settings or configuration of the affected equipment or software;
- b. Recommending the purchase of upgrades, or procurement of supplemental or addition equipment or software;
- c. Coordinating with your contracted service providers as necessary;
- d. In cases where no comprehensive remedy is known or available, provide guidance as to how to minimize the occurrence and impact of adverse Health and Status events.

Why This Service Is Useful: This service provides the foundation for proactive remediation of covered equipment and software problems. Equipment and Software may report problems occurring for prolonged periods before the user is aware of an impending failure. This service enables IU to sense, diagnose, and react to potential problems all with minimal disruption of the affected users.

HELPDESK SERVICE: IU maintains a help desk for managing a tracking your service requests. You may request help through the Helpdesk via voice, email, fax, or other convenient means. IU tracks the status of the Helpdesk Request and updates the requestor throughout the lifecycle of the request.

Why This Service Is Useful: By providing centralized registration and tracking of Helpdesk Requests, you have a consistent and reliable way of reporting and requesting updates on requests. The centralized helpdesk is also useful for tracking trends and for efficiently communicating with groups of users affected by a service issue.



Information Understructures

MALWARE MANAGEMENT SERVICE: IU monitors your anti-virus, anti-spam, and other anti-malware software or services installed on your equipment. IU monitors the following events or conditions:

- a. The currency of anti-virus signatures or definitions;
- b. The operating status of anti-malware programs;
- c. Scan histories and events;
- d. Threat histories and events;
- e. Status of anti-virus subscriptions;
- f. Detected malware penetrations of Client's system.

In addition, IU performs the following tasks in connection with the Malware Management Service:

- a. Report malware penetrations to you;
- b. Perform the administrative efforts necessary to renew anti-virus subscriptions and license renewals;
- c. Provide monthly tunings of anti-spam software;
- d. Management of malware quarantine areas;
- e. Effort to attempt remote repair or remediation of malware damage. IU cannot assure that malware penetrations are detected or predicted. IU does not assure penetrations can be remediated remotely, or remediated at all without a substantial on-site rebuilding effort. Remediation efforts that cannot be performed remotely are not provided for under this service.

Why This Service Is Useful: Attacks through viruses, spam, or other malware are among the most prolific and damaging risks to computer operations. This service enhances the detection and mitigation of malware attacks.

ON-SITE INSPECTION SERVICE: IU performs onsite inspections of your facilities for the purpose s of:

- a. Performing a supplemental tape drive cleaning if appropriate;
- b. Inspecting the physical condition of your covered equipment and software;
- c. Identifying factors that could affect the reliability, availability, and security of your information system;
- d. Interacting with your staff to discern impediments to effective operations and opportunities for improvement;
- e. Updating IU's documentation of your environment, covered equipment, and software.

Why This Service Is Useful: While many services are best performed remotely and unobtrusively, a periodic visual inspection can expose threats to effective and reliable operations, and gaps or weaknesses in the services being provided. This service adds to the comprehensiveness of IU's services by providing a visual inspection.



Information Understructures

PATCH AND UPDATE SERVICE: IU remotely supervises or performs the installation of patches and updates including:

- a. Updates for Microsoft branded covered equipment and software;
- b. Service Packs for Microsoft branded covered equipment and software;
- c. Patches for Microsoft branded covered equipment and software;
- d. Updates, Service Packs, and Patches (or their equivalents) for non-Microsoft branded covered equipment and software and intended by the manufacturer to be installed by end-users via internet download obtainable:
 - i. Without charge for properly licensed users;
 - ii. Via subscription or maintenance plan paid by Client;
 - iii. Via fee-for-download paid by Client.

IU does not provide the following under Patch and Update Service:

- a. Installation of upgrades or hot fixes to software products covered under this agreement;
- b. Installation of alternate, replacement, or successor software products to those covered under this agreement;
- c. Installation of updates, service packs, or patches that cannot be installed via IU's remote connectivity capabilities.

Why This Service Is Useful: The consistent application of patches and updates is an important task for maintaining the availability, reliability, and security of your information systems. It can also be the most time consuming. Even small networks of only a dozen or so computers can require hundreds of patch and update activities each month. Under this service, IU performs patch and update services.

REMOTE SUPPORT SERVICE: This service remotely supports Helpdesk requests. Through this service, IU makes remote connection to your affected equipment or software to provide service. This service may require the installation of agent software on your equipment.

Why This Service Is Useful: Remote Support Services is an advanced alternative to traditional on-site service. This service permits faster response, less intrusive repair actions, reduced cost, and improved staff productivity.



Information Understructures

REPAIR MANAGEMENT SERVICE: IU manages the repair of your covered equipment, software, or service failures. This service includes:

- a. Identification of defective or failing equipment, software or service;
- b. Coordination of repair activity with an appropriate vendor;
- c. Supervision of on-site repair activity;
- d. Efforts to pack, ship, receive, and re-install your equipment that is repaired or replaced via the repair vendor's offsite facility or shipping point.

Why This Service Is Useful: Your equipment and software vendors may require you to participate in a disruptive and time-consuming troubleshooting process. You may also be required to coordinate with vendor service personnel, and may be responsible for shipping and receiving failing or repaired equipment. This service shifts all such coordinating activity to IU relieving you of the administrative burden associated with vendor service activities.

SYSTEM ADMINISTRATOR REPORT: IU provides a report monthly via email detailing the following items:

- a. A summary of Helpdesk Request activity;
- b. A summary of Patch and Update activity;
- c. A summary of system Health and Status activity;
- d. A summary of backup audit findings;
- e. A summary of malware activity;
- f. A summary status of repair activity;
- g. A summary of walk-through findings (when applicable);
- h. A summary of security and account activity;
- i. A statement of accumulation and usage of the Technical Reserve.

Why This Service Is Useful: This service provides the Client's management with a top-level view of operational issues and events related to the Client's information system.



TECHNICAL RESERVE SERVICE: Technical Reserve is technician time that accrues each month to perform services requested by you that are not specifically provided for under another service. Technical Reserve time accrues at the rate of 1 hour/month per covered physical server and ¼ hour/month per covered physical workstation. We provide Technical Reserve time in increments of ¼ hour with a ¼-hour minimum for remote service, and a 1-hour minimum for on-site at your facility. Unused Technical Reserve rolls over from month to month. Unused Technical Reserve expires at the termination of the agreement. You may not use unused Technical Reserve as payment for any outstanding invoice.

Why This Service Is Useful: This service provides a capacity to address your requests for occasional special service or attention without incurring costs or the administrative burden of initiating a purchasing request.

ⁱ Windows Server 2003 / Windows Server 2008 are capable of performing several organic server roles without the need for additional software. For example: DHCP Server, DNS Server, Domain Controller. When a server is configured to perform these core roles, and only these core roles, we define such a server as a “Core Role” server.

ⁱⁱ Windows Server 2003 / Windows Server 2008 are capable of supporting additional members of the Microsoft Server family such as Exchange Email Server, or Microsoft SQL Server. When a server is configured to support these additional roles, we define such a server as an “Extended Role” server.

ⁱⁱⁱ ‘P’ denotes a server running on actual physical hardware.

^{iv} ‘V’ denotes a server running on a virtual hardware platform, typically as a guest operating system.

^v Email Management Service on a Small Business Server is limited to the integrated version of Microsoft Exchange Server delivered as a component of Small Business Server.

^{vi} Email Monitoring Service on a Small Business Server is limited to the integrated version of Microsoft Exchange Server delivered as a component of Small Business Server.

^{vii} SQL Server Management on a Small Business Server Premium Edition is limited to the integrated version of Microsoft SQL Server delivered as a component of Small Business Server Premium Edition.

^{viii} ISA Server Management on a Small Business Server Premium Edition is limited to the integrated version of ISA delivered as a component of Small Business Server Premium Edition.