



ICT SOLUTION and SERVICES

1. End User Computing (Desktop)

1. **Thin Client Technologies, Terminal Services, VDI** that adapt varying bandwidths and network latencies whilst remaining capable of streaming to devices. Solution and service capability encompasses:
 - Application Desktop & Content Publishing;
 - Seamless Windows session sharing;
 - Desktop SOE development & integration;
 - Web Interface and SharePoint;
 - Universal Print Driver;
 - USB Redirection;
 - Multi-monitor and expanded screen resolution;
 - Bi-directional audio;
 - Latency reduction;
 - Multimedia and Graphics acceleration;
 - Automated virtual desktop provisioning.
2. **Desktop provision:** Project based or delivered as a managed service.
3. **Virtual Desktop Infrastructure (VDI):** VDI combines all of the benefits and flexibility of server virtualisation with the power and personalisation of traditional desktop computing. VDI virtualises a desktop image that is deployed from a centralised server. The solution delivers an organisation reduced operating costs, improved security, and consistent familiar end-user experience with little to no learning curve.
4. **Desktop Support:** warranty management, replacement of faulty equipment, return to manufacturer for repair and return to pool, printer access, and printer support.
5. **Desktop SOE:** development, deployment, patching, applications interoperability testing and optimisation, support of standard notebook configurations, mobile home user support.

2. Infrastructure (server, network, storage, firewall)

1. **Asset Discovery & Management:** automated inventory and update of connected devices.
2. **Load Balancing:** dynamic reassignment of resources to applications based on optimal resource allocation based on point in time user demand.
3. **Monitoring and Management:** automated verification of infrastructure operation with dynamic problem identification, diagnosis and initiation of corrective action.
4. **Orchestration** – provisioning based on actual workloads with the ability to de-provision, re-provision, and apply optimised infrastructure assets (processing, storage, network) on demand.
5. **Provisioning:** synchronised infrastructure provisioning and configuration (processing, storage and network).
6. **Utilisation Monitoring:** monitoring of infrastructure resources to meet SLA and provide the foundation for chargeback.
7. **Virtualisation:** HW, SW and para-virtualisation to support multiple applications sharing a physical infrastructure asset or a single application supported by a pool of infrastructure assets for higher performance. Reduction of servers delivering operational savings i.e.: reduced physical housing, HVAC and power costs. Increased workload per server delivering higher user density and utilisation per device. Dynamic load balancing between virtual servers and in situ re-assignment of applications between virtual servers.
8. **Integration with multiple hypervisors:** VMware and HyperV.
9. **Server Based Replication, Provisioning & Recovery:** Data replication from one server to another through automation and workflow without degradation in network performance or end user impact.
10. **Server Provision:** project based or delivered under a managed service.
11. **Server Performance Management:** monitors server availability and performance utilising over 300 server performance metrics including CPU utilisation, partition-wise disk space, memory utilisation, processes, thru to individual device environmental status. Service includes pre-configured health monitoring for Dell, HP & IBM servers with SNMP, WMI and CLI (Telnet/SSH) based monitoring of other vendor devices.

General Enquiries	Technical Support	Accounts	Sales	Feedback
info@mbits.com.au 02 6163 2400	techsupport@mbits.com.au 1300 887 565	accounts@mbits.com.au 02 6163 2400	sales@mbits.com.au 02 6163 2400	feedback@mbits.com.au



12. **LAN/WAN Provisioning & Management:** data carriage, provision of network links, secure data transmission, encryption, routing, switching, Firewall/VPN, IDP, IDS active/active, WAN acceleration, dashboard, real time event monitoring, software distribution, network fault monitoring and diagnosis.
13. **LAN/WAN Device Management:** device management using tools including ICMP Ping, Trace Route, Remote Desktop Session, Telnet, SSH session. Features display of traffic in real time, monitoring and management with device performance graphing.
14. **Network Availability Monitoring & Management:** proactive performance management, capacity threshold alerting, system administration, trend ICMP, SNMP traps and Syslogs from network devices with alerting by email, SMS. Automated logging of incident and creation of an Incident in the Service Desk system. Circuit IDs of links, network visualisation, contact details and escalation points are stored centrally to reduce throughput time in addressing link and device related issues.
15. **Network Utilisation:** threshold mapping, decision support, trend analysis, capacity planning and management.
16. **WAN Latency Management:** utilising IPSLA technology, trouble-shooting of WAN RTT problems through accurate identification of high latency network devices and paths.
17. **WAN Traffic Analysis:** visibility of the traffic passing through and across the WAN. Identifies which user or application is generating the highest traffic, traffic prioritisation, WAN bandwidth management and identification of traffic from applications such as SAP or Siebel that use dynamic ports.
18. **Network Change & Configuration Management:** reduces the frequency and impact of network outages and performance issues through automated configuration management and update of network devices.
19. **Remote Site Monitoring & Management:** a device deployed at each site performs all the network-facing capability such as discovery, mapping, fault monitoring with reporting back to the central server located at either the NOC or Data Centre. Ping and TraceRoute requests can also be executed within the probe from the central server to allow problem diagnosis and resolution at remote sites. Any service pack upgrades performed on the central server are automatically pushed to the remote devices.
20. **ESX Server & VM Instance Management:** monitoring dashboard for each ESX server providing real-time information on CPU, memory and disk utilization for each of the guest VM instances running. The dashboard report shows the different VM instances on the ESX Server, highlighting the status of each instance. Monitored resources and parameters include: allocated system resources, percentage of resources utilized CPU, Memory etc, the Disk I/O, Network I/O, the traffic sent out or received through the virtual Ethernet network and storage adapters (VMnic and VMnet). The service also provides options to Start, Stop and Suspend VM instances running on the ESX server with alert generation should a VM be consuming excessive resources with the facility to remotely stop or suspend a VM when required.
21. **File and Print** – clustering, active active, active passive, antivirus, roaming profile, user storage management, shared file storage management, user authentication, permission management, backup, restore disk and tape.
22. **Intranet Access** – content management, migration of existing Intranet sites, Bitmap acceleration, SharePoint integration, Patch management, antivirus, backup, user account management, security permissions.
23. **Active Directory** – AD management, health monitoring, issue identification and resolution, high availability solution design.
24. **Application Performance Monitoring & Management** - ensures end users access to applications is optimised and decision based support can be delivered in diagnosis of performance related problems. Monitoring of response times for applications and databases inclusive of dashboards and pre-configured monitors for MS Exchange, MS SQL and Active Directory. Monitoring capabilities (include but not limited to) Windows Servers, Exchange Server, Active Directory, SQL Server and other customer specific applications in providing visibility upon which informed decisions and corrective action can be taken.
25. **Remote Support** – Terminal Services Shadowing, Daneware and Remote Desktop take-over delivered through the Service Desk in conjunction with the Network Operations Centre.
26. **On-Site Support** – thru partner support network covering all states and territories, city, regional and remote locations Australia wide.
27. **Proactive Maintenance** – threshold monitoring, capacity management, utilisation reporting, trend analysis and decision support for server, storage and LAN connectivity, emergency change, preventative maintenance based on agreed scheduled maintenance windows.

General Enquiries	Technical Support	Accounts	Sales	Feedback
info@mbits.com.au 02 6163 2400	techsupport@mbits.com.au 1300 887 565	accounts@mbits.com.au 02 6163 2400	sales@mbits.com.au 02 6163 2400	feedback@mbits.com.au



3. Secure Internet Enterprise Gateway Environment (SIEGE)

SIEGE is a fully managed service designed owned and operated by mbits, physically housed in the mbits Data Centre and supported by the mbits Service Desk and NOC located in Queanbeyan.

SIEGE is a state of the art secure gateway service currently in its 3rd Generational Release.

SIEGE features:

- Dual100Mbps high availability diverse path redundant connectivity;
- Data Centre rated T4 to PROTECTED by ASIO;
- Secure web and server hosting;
- email gateway services;
- Internet services;
- Secure firewall services and remote access;
- Unified Threat Management;
- Gateway Applications Management ;
- Centralised Policy Management;
- Change management;
- IPV6 support;
- Forward proxy;
- Network visualisation;
- Shared physical network with logical user separation;
- Traffic identification, management by protocol & application down to the end user;
- WAN optimisation - reduced network latency, optimised application performance;
- Prioritisation of traffic with demand moderation;
- Intrusion Protection (IPS), Intrusion Detection (IDS);
- Single pass architecture - inline security, no system performance degradation;
- Content filtering;
- Continuous vulnerability assessment;
- User Activity Monitoring & Management - User-ID enables policy control over applications and content based on the user or group identity through seamless integration with Microsoft Active Directory. Performs analysis on application, threat and web surfing activity based on an individual or group of users. Identify users and apply policy controls over their respective application usage. Build and deploy policies to enable application usage for specific groups or Departments.

4. IP Telephony (VoIP), Video Conferencing, Unified Communications

1. **Unified Communications:** for convergent support and integration of communications including secure instant messaging, email, IP telephony, video conferencing.
2. **VoIP Performance Management:** commences with VoIP readiness testing, monitoring VoIP performance, through to troubleshooting VoIP call quality.

5. Secure Authentication & Remote Access (SyferLock)

1. Token less 2 factor authentication: no token required;
2. Higher security through inclusion of decoy digits;
3. Reusable one time password (OTP);
4. User never actually types the password in;
5. User can change the password without Service Desk or System Administrator assistance;
6. Zero client side footprint: no modification to existing Desktop SOE;
7. End User administration and activity logging;
8. Users can use their existing passwords;
9. Service providers can maintain their existing infrastructure for account management;

General Enquiries	Technical Support	Accounts	Sales	Feedback
info@mbits.com.au 02 6163 2400	techsupport@mbits.com.au 1300 887 565	accounts@mbits.com.au 02 6163 2400	sales@mbits.com.au 02 6163 2400	feedback@mbits.com.au



10. Supports all requirements involving the authentication of users before they interact with mission-critical data and applications through Remote Authentication (SSL VPN), Intranets & extranets, E-mail, Microsoft Windows etc;
11. Scales to millions of users;
12. Alternative to federated identity without the need to share database information or synch databases;
13. Supports multiple languages and character sets: users into information in their native language.

6. Cloud Computing

1. **Cloud Computing:** secure Private & Public Cloud computing delivering on demand access to computing resource (servers, network, storage, applications and services), rapid provisioning, supported, managed with data backup recovery and retention as per Federal Government policy.
2. **Infrastructure as a Service (IaaS):** short medium or long term provision of infrastructure through hosting for DR, IT Service and Business Continuity, Development, Test, Training, Pre-production, Application Modelling, Capacity Planning, System Performance Assurance, Web Site/Portal development.
 - a. server virtualisation;
 - b. storage;
 - c. Firewall;
 - d. secureLAN;
 - e. database;
 - f. Secure Internet Gateway (SIEGE);
 - g. VPN and remote access;
 - h. email archiving;
 - i. content management;
 - j. backup and restore.
3. **Software as a Service (SaaS):** short medium or long term provision of software, specialist applications and associated delivery infrastructure on demand and billed on an as used basis.
 - a. TenderingBITS (specialist application);
 - b. Email;
 - c. SharePoint;
 - d. Admin Portal (specialist application);
 - e. Website;
 - f. Internal/DMZ.
4. **Data Security:** - file storage encryption (data at rest) integrated with Digital Rights Management (data on the fly). Hierarchical storage management to automate movement of data and files under centralised group policy.
5. **Bespoke Development: Tender Management Software Application (TenderingBITS).**
Web based application developed by mbits to significantly reduce the resource, cost overheads and streamline the process in managing and responding to a RFT, EOI or RFP. The customer (Tender Issuer) takes a service for the duration of the process. At conclusion of the engagement all data is provided to the customer on CD for audit & data retention purposes and the environment is removed.

The application is currently in its 4th release and has been developed from inception by mbits to be fully compliant with Commonwealth Procurement Guidelines (CPG), the Information Security Manual (ISM) and Protective Security Manual (PSM). The application features:

- Centralised Virtual Data Room;
- Collaboration & communication between tender issuer and tender respondents;
- Question & Answers;
- Anonymous Interaction;
- Document Security – multiple formats, AES Encryption, Digital Rights Management;
- Rapid Deployment ;
- Scalability;
- Compliant – ISM, PSM & Commonwealth Procurement Guidelines;
- Respondent Registration facility;
- Pre-configured workflow for approvals, reminders and customised KPI's;
- Standardised approval templates with rule based workflow;
- Centrally managed database structure;
- Process governance – audit logging;

General Enquiries	Technical Support	Accounts	Sales	Feedback
info@mbits.com.au 02 6163 2400	techsupport@mbits.com.au 1300 887 565	accounts@mbits.com.au 02 6163 2400	sales@mbits.com.au 02 6163 2400	feedback@mbits.com.au



6. **Bespoke Development: Administration Portal**

Delivers automated self administration of Active Directory accounts, specifically:

- Update user details;
- Create new account;
- Modify or Unlock account;
- Reset password;
- Add to or remove from security group;
- Add to or remove from distribution list;
- Create new Group or delete group;
- Disable account until date;
- Enable or delete an account;
- Immediately delete account.

7. **Portals:** delivering a single point of access to applications using web based user interface technologies. Developed by mbits and integrated into the TenderingBITS solution and Private/Public Cloud (IaaS, SaaS) offerings.

8. **Mashup technologies:** rapid delivery of specialist applications to end users, and integrated into the TenderingBITS, SIEGE, portal and Private Cloud (IaaS, SaaS) offerings.

9. **Digital Rights Management:** controlled access to data including prevention of access, copying, printing, screen scraping or conversion to other formats for unauthorised dissemination of information to others. Integrated into the TenderingBITS solution and Private/Public Cloud (IaaS, SaaS) offerings.

7. Delivery Infrastructure & Cross Platform Services

1. **Service Desk:** Located in Federal region and staffed by permanent mbits employees. Service Desk is ITIL compliant. Customer access via online services portal, email or toll free 1800 number. Service request, service restoration, end user knowledge base, commonly asked questions, fixes, help and issue remediation. SLA measurement, management and reporting, problem resolution, escalation, service restoration, root cause analysis with remediation. Management services include, incident, problem, configuration capacity, change, release, asset inventory, software licencing, service continuity.
2. **Network Operations Centre:** Located in Federal region, staffed by permanent mbits employees. Integrated with the Service Desk in delivery of proactive systems management, alert monitoring, security management, application performance and usage monitoring, patch management, remote troubleshooting, performance tuning, capacity management and problem resolution.
3. **Data Centre:** The mbits Data Centre is located at 470 Northbourne Ave, Canberra ACT 2601. The mbits Data Centre Facilities are N+1 and rated Type 1 under Australian Standard 2834/1995 incorporating redundant cooling, dual generators and dual UPS. The Data Centre meets the requirements of TIA-942, as a Tier 3 data centre (concurrently maintainable) with much of the infrastructure meeting Tier 4 standards. Service delivery Infrastructure and customer environments are physically housed inside SCEC endorsed B Class racks, inside an intruder resistant Data Centre facility protected by a Type 1 security alarm system.
4. **Hosting/Virtual Data Centre:** Infrastructure as a Service (IaaS), short medium or long term hosting for DR, IT Service and Business Continuity, Development, Test, Training, Pre-production, Application Modelling, Capacity Planning, System Performance Assurance, Web Site/Portal development.
5. **Service Delivery Management:** service levels, service desk, incident management, problem management, change & release management, availability management, backup and archive, configuration management, security management, capacity management, network operations, project reporting.
6. **Contract Management:** financial management and reporting, resource management, 3rd party licence, hardware, software and application licence management.
7. **Virus Prevention & Protection:** encompasses all incoming and outgoing data, email and web traffic. Protection against viruses, spyware, hacker attacks, phishing and spam. Proactive protection from new malicious programs covering mail servers, file servers, scanning of web traffic in real time. Quarantine of infected workstations, blocking of virus epidemics, centralised reporting, centralised installation and management, support for hardware proxy appliances and automatic updating of databases.
8. **Storage Management:** centralised, high availability redundant RAID, clustering, thin provisioning, snap shooting, remote copy, provisioning of storage space and data storage resources including backup media. Optimisation services, data availability ensuring sufficient storage for database recovery, database tuning, application testing and training. Monitor and report on storage space utilisation, reliability, issues and recommendations for improvement.

General Enquiries	Technical Support	Accounts	Sales	Feedback
info@mbits.com.au 02 6163 2400	techsupport@mbits.com.au 1300 887 565	accounts@mbits.com.au 02 6163 2400	sales@mbits.com.au 02 6163 2400	feedback@mbits.com.au



9. **Backup, Archive and Restoration Management:** perform, monitor and retain backups of all data, business applications, system, transaction, security logs. Re-run backups when required, label backups, store backup media in offsite fireproof storage. Maintain supply of backup media, manage media disposal, retain in accordance with the Archives Act 1993 or other data retention policy.
10. **Project Services** – provide proposals, prepare project management plans, implementation, delivery and post implementation support. Services include but not limited to systems installation, desktop & notebook refresh, remote access & secure authentication, wireless solutions, IaaS, SaaS, SIEGE, VDI (thin client/terminal services provision), VoIP, Video Teleconferencing, email archive, Content Management, System Staging and Implementation.
11. **Data Migration and Service/Infrastructure Transition** - develop and deploy implementation plans for customer data migration, service transition, implementation, post implementation support, risk management & mitigation, end user training and services lifecycle support.
12. **Services Reporting** – specific to each client and delivered monthly in person. Typical reporting includes service levels, service desk, incident management, problem management, change & release management, availability management, backup and archive, configuration management, security management, capacity management, network operations, project reporting.
13. **Capacity Management** – system performance and capacity report against agreed thresholds for all Infrastructure and storage components. Response to thresholds breaches due to incidents as a result of insufficient capacity. Commentary on ability of the infrastructure to meet required system performance, service levels including trend reporting.
14. **Data storage and security** Shared storage and backup architecture enabling rapid deployment across all areas of business operations utilising one security framework and common process.

8. Professional Services

1. **Network Architecture Design and Installation** – Thin client, terminal services, VDI, Server consolidation, HW, SW virtualisation, WAN, LAN, Security, Storage, email archiving, content management, VoIP, Video Conferencing, Backup, Recovery, DR, BCP and IT Service Continuity .
2. **System Architecture Design** - review, preparation, presentation and compliance assessment against applicable policy and standards: ISM, PSM, AN/NZS 7799.
3. **Operations Assessment** - audit and risk studies that include a comprehensive analysis of capacity, performance levels, contingency, business continuity, threat, vulnerability and security planning. The output of this service is a report and presentation of findings, issues, recommendations and suggested mitigation strategies.
4. **Services Planning** – provide input into our customers IT planning and budget preparation process to provide cost certainty, IT spend forecasts, maximise IT investment aligned to business need and assist in supporting the organisations IT strategic direction.
5. **IT Services Continuity and Disaster Recovery** – comprehensive risk analysis DR service provision inclusive of DR assessment, DR planning, DR plan preparation, DR running and participation in DR testing.
6. **Database & Applications** - maintain the database environment to ensure stable, well tuned and efficiently managed customer database and application environments. Includes upgrades, patches, disk quotas, memory, batch and print queues, performance monitoring, backup, restore, monitor system server logs, scheduled and emergency maintenance.
7. **IT System Compliance Assessment & Review** – review and assessment against ISM, PSM, AN/NZS 7799 and other information and data communication standards applied across Federal Government.
8. **Network Security** – audits, vulnerability assessment, penetration testing, security policy review, regulatory compliance assessment against ISM and PSM.

General Enquiries	Technical Support	Accounts	Sales	Feedback
info@mbits.com.au 02 6163 2400	techsupport@mbits.com.au 1300 887 565	accounts@mbits.com.au 02 6163 2400	sales@mbits.com.au 02 6163 2400	feedback@mbits.com.au