Follow-up to IS Usage Guideline Workshop

IS Usage Guideline Version 1.1

Technohaven – IBCS-Primax Consortium

16 July 2017

16 July 2017

Engr Mostafa Kamal,
Project Director,
Second Rural Transport Improvement Project (RTIP II),
Local Government Engineering Department (LGED),
LGED Bhaban, Agargaon, Dhaka

Subject: Follow up to IS Usage Guideline workshop at Hotel Lakeshore dated 27 April 2017

Dear Sir,

Please recall that in our '**Key Deliverable 2 (KD2)'** we recommended an Information Systems (IS) Usage Guideline for LGED. A high-level IS Usage Guideline workshop was held on 27/04/2017 at Lakeshore Hotel where some policy level as well as operational level suggestions were provided by the LGED participants.

A follow-up meeting was held with the LGED GIS and IT Unit on 01/06/2017 to review the technical aspects of the IS Usage Guideline.

In line with the suggestions provided in the workshop and the review meeting we are enclosing herewith the following documents for the needful at your end:

   a.   Brief on actions taken as per suggestions provided
   b.   Updated IS Usage Guideline for LGED
   c.   Annexures for reference

We look forward to your confirmation of subsequent workshops on formal adoption of the IS Usage Guideline throughout all offices of LGED.

With best regards,

(Habibullah N Karim)
Team Leader
Technohaven – IBCS-Primax Consortium

Follow-up to Revised ICT Strategy and Action Plan

Information Systems Usage Guidelines Version 1.1

Information systems (IS) have to incorporate efficient configuration of their facilities and management methods to survive in today's rapidly changing environment. Therefore, there is a growing need for information systems that are both highly productive and flexible. Higher productivity lowers service delivery costs and higher flexibility helps in overcoming various uncertainties regarding the volume and attributes of information resources. Such efficient utilization of IS resources requires adherence to some basic principles and common-sense approach to security and fail-safe operation which are compiled here as "LGED Information Systems Usage Guidelines (LISUG)". The LISUG is organized into a dozen sections as shown below based on IS operational needs. The number of sections can be amended as per operational prioritizations. The proposed sections are:

(A) Enterprise-Wide Applications
(B) Individual Productivity Applications
(C) Data Storage and Backup
(D) Workstations and End-user Devices
(E) Use of Internet
(F) Internet Security
(G) Use of e-Mail Systems
(H) Use of External Media
(I) Use of Hardcopy
(J) Request for Services
(K) Outsourcing services to vendors
(L) SLA (Service Level Agreements) with vendors
(M) E-WASTE DISPOSAL POLICY

(A)   Enterprise-Wide Applications:

Overview:

Enterprise architecture looks at the strategies, functions, processes, data, systems, organizations and people of an enterprise in order to better align resources with the strategic objectives of the organization. It provides an enterprise-wide

functional view of an organization which reduces redundancy and promotes a shared view of data and processes across the organization. This, in turn, reduces the complexity of the IS environment, improves reliability, and reduces costs. When an organization's quality improvement process begins generating benefits, such as cost savings and improved efficiency, the next step is clear: expand the scope of the successful program to derive all of the positive returns possible. To do so, an organization must include everyone in the process. And to that end, many are turning to enterprise-wide applications.

Recommendation:

1. Enterprise architecture is set as standards for the design of new systems and the strategic direction for implementing **custom built enterprise-wide applications for LGED** such as IDSS, uFMS, PIMS and ePMS Etc.
2. All enterprise applications be installed in a central data center.
3. All users to have round the clock access to enterprise applications at the data center.
4. System administration, maintenance and operational support of enterprise applications to be centrally managed resulting in consistency and reliability in day to day operation.
5. The IS Unit shall set the standards and manage the support needs for enterprise applications.

Adoption:

The knowledge and experience built up within the organization should be used and communicated widely. Digital technologies rapidly change while more services will gradually become digitalized. So, based on needs, LGED may consider the following adoption protocols:

1. All enterprise-wide applications shall be web-based, which requires only a computer with an Internet/network connection and a Web browser for using the applications. Such applications are not bound by local-area-networks and so the distance between the user and the central repository of data is immaterial. Web-based applications are also platform independent i.e., all types of devices from smart phones, and tablets to PCs and laptops running any OS should be able to access the enterprise applications.
2. All applications that are meant for use across the organization need to be declared "Enterprise-wide Applications" and these shall be maintained at the Data Center as web-based applications.

3. The IS Unit shall administer and maintain all enterprise applications.

(B) Individual Productivity Applications:

Overview:

Productivity application is an application software dedicated to producing information, such as documents, presentations, worksheets, databases, charts, graphs, digital paintings, electronic music and digital video. Its name arose from the fact that it increases productivity, especially of individual office workers, from typists to knowledge workers, although its scope is now wider than that. Any program used to create or modify a document, image, audio/video clip is a productivity application.

Recommendation:

Productivity applications traditionally run directly on a computer. These applications are the reasons people use personal computers. Productivity applications help a professional or a common user to enhance and complete their tasks expeditiously. For such applications the general guideline should be:

1. Business applications such as AutoCAD, ArcGIS, ETABS, Microsoft Office, and others which are not centrally procured and administered, can be installed locally on a user's PC or laptop.
2. All user data (document, image, audio/ video clip) to be saved on individual PC or laptop. All such data (except personal use data) to be synchronized with a backup directory at the Data Center.
3. As far as possible all users shall use the same version of individual productivity applications. The IS Unit's assistance can be sought regarding this.
4. Users shall make best efforts to ensure appropriate license for any application installed on his/her PC.
5. If any user has data which are relevant for other users then those data shall be copied to the public/shared directory at the central data center.

Adoption:

The adoption rules for productivity applications can be:

1. Office productivity – MS-Office version 2010 or later
2. Design – AutoCAD ver. 2016 or later / Adobe Illustrator ver. 15 or later

3. GIS – ArcGIS version 10.5 or later
4. Civil Engineering – ETABS ver 2016 or later / STAAD.Pro ver 8i SS6 or later

5. Social Media applications such as Facebook, Twitter, LinkedIn and others hamper productivity when used in unrestrained fashion and hence their use may be allowed under IS Unit's guidance.

(C) Data Storage and Backup:

Overview:

In this age of information an organization's success is tightly coupled with its ability to store and manage information. Data storage systems provide a critical part of an organization's network infrastructure. With the amount of data growing at an ever increasing rate the data storage strategy is critically important for a modern organization.

Recommendation:

1. Individual workstations need to segregate office-use and personal-use data under separate directories.
2. Office-use data need to be synchronized with a backup directory at the data center daily.
3. Movies, songs and other entertainment data must not be saved in the office-use directory and in the backup directory at the data center.
4. All data files shall be saved conforming to the file-naming conventions in use.

Adoption:

Process and protocols to be used:

1. Instruct all users to scrutinize their individual workstations and segregate office-use and personal-use data under separate directories with a firm deadline (say 1st Jan 2018).
2. Train all users how to synchronize office-use data with the backup directory at the Data Center.
3. Train all users on file-naming conventions.

(D)   Workstations and End-user Devices:

Overview:

In today's mobile workplace, employees need the ability to access data and applications from anywhere. From tablets to desktop computers, and mobile phones to handheld scanners, the organization's information infrastructure needs to support a multiplicity of end user devices (EUD) to access enterprise resources. However, there is a need for some discipline in the extent of allowable EUDs and environments to ensure consistent look and feel as well as operational integrity of applications.

Recommendation:

1. Allow "Bring Your Own Device (BYOD)" flexibility in policy but specify the BYOD policies and procedures. This will save capital expenditure for hardware and software and related IS operational expenses. It will also boost user mobility and productivity as well as provide a strong differentiator in retaining talent.
2. All workstations shall conform to a minimum standard specification and configuration. The workstation standard should be circulated to all users by the IS Unit and should be updated every year in July.

Adoption:

It is critical for organizations to analyze key factors related to security policies, delivery model, IS solutions and support structure in order to define an effective device-agnostic EUD strategy.

The minimum specifications and configurations to be adopted:

SW / HW→ ↓	PCs/ Laptop	Tablets/ Smartphone	Standalone Servers
Operating System	Windows 7/8	Android 4.4/ iOS8	Windows 2012 server
Processor Type	Core i3	-	Core i5
RAM	4GB	1GB	16GB
Storage	200GB	16GB	3000GB
Microsoft Office	MS Office 2010/2011/2013	MS Office 2010/2011/2013	MS Office 2010/2011/2013
Internet Tools	**Browsers:** Mozilla Firefox 32, Internet Explorer 9, Chrome 37; or later	**Browsers:** Mozilla Firefox 32 or later, Safari 8 or later	IIS with a real IP address
File Exchange Format	**Text:** ASCII, MS-Word (.doc), RTF; **Graphics:** GIF, JPEG, PNG image formats; **Archives:** ZIP, Auto-extract	**Text:** ASCII, MS-Word (.doc), RTF; **Graphics:** GIF, JPEG, PNG image formats; **Archives:** ZIP, Auto-extract	**Text:** ASCII, MS-Word (.doc), RTF; **Graphics:** GIF, JPEG, PNG image formats; **Archives:** ZIP, Auto-extract
Virus and spyware protection software	MacAfee/Kaspersky/ Other Antivirus	MacAfee/Kaspersky/ Other Antivirus	MacAfee/Kaspersky/ Other Antivirus
E-mail	SMTP/Webmail	SMTP/Webmail	SMTP/Webmail
LAN Card and redundancy	100Mbps or higher LAN card with Wi-Fi support	Wi-Fi and 3G support	100Mbps or higher LAN card with Wi-Fi support and another LAN card for the real IP; 3 x 1000GB HDD in RAID 5 configuration

(E)   Use of Internet:

Overview:

An [internet usage policy](#) provides employees with rules and guidelines about the appropriate use of IS equipment, network and Internet access. Such a policy helps protect both the organization and the employees.

Recommendation:

Users shall have access to Internet services under the following principles:

1. Information available to the public on the Internet shall also be available to users, especially those involved in the delivery of associated services. But all Internet users shall be provided with this document and shall be required to acknowledge these guidelines when obtaining Internet access. These are best practices that apply to use of the network in general and are part of organizational security precautions.
2. Access limitations shall be dictated by system and network bandwidth availability and need.
3. The users need to be aware that browsing certain sites or downloading files from them is prohibited due to security reasons. Users shall be individually liable for any negligence in this regard.

Adoption:

The Internet Usage Policy is an important document that shall be read and acknowledged by all employees once a year to ensure any changes in the security directives and general advisories.

1. Users shall not use the network for private business or solicit money for personal causes or network for political lobbying.
2. Users shall refrain from any malicious use of the network and/or spreading programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system.
3. Users shall not use the network to access or process pornographic and/or other morally offensive materials. Use of abusive or derogatory language in either public or private messages is prohibited.
4. Users shall conform to the rules of etiquette or established usage policies for each of the available Internet services.

5. Users shall respect intellectual property rights at all times when exchanging information over the Internet.
6. Users shall follow accepted information management policies and procedures for Internet documents.
7. Users shall respect and follow the provisions of the ICT Act 2015 regarding online etiquette.

(F)   Internet Security:

Overview:

The Internet represents a diversified tool that offers great benefits to the users and to the organization. Unfortunately, Internet can also divert attention from productive work practices and heighten security risks if not used properly.

Recommendation:

1. Inappropriate use of Internet resources can increase the organization's exposure to liability and make the networks more vulnerable to hackers, virus infections, and other dangers.
2. Users are expected to use the Internet responsibly and productively. Internet access shall be limited to job-related activities only.
3. All data that is composed, transmitted and/or received by organization's computer systems shall be considered the organization's intellectual property (IP) and recognized as part of office-use data.
4. The equipment, services and technology used to access the Internet are the property of the organization and the IS Unit reserves the right to monitor Internet traffic and take preventive measures if any user is found deviating from the usage policies.
5. Emails shall not contain content that is deemed to be offensive.
6. All sites and downloads may be monitored and/or blocked by the IS Unit if they are deemed to be harmful and/or not productive to business.

Adoption:

1. The passwords shall contain minimum 8 digits including at least one each of upper case, lower case and numeric characters.

2. Accessing remote systems to download data and executable files shall be done only for sites which have valid security certificate or are known to the user to be authentic. Any such files may have been infected by a computer virus or contain a malicious software code that might destroy data files, copy password files, or negatively affect the local area network. Any file downloaded from the Internet, whether a data or an executable file, must be scanned for viruses automatically prior to its use. LGED maintains a licensed copy of MacAfee anti-virus software centrally that is available to all employees. However, the IS Unit may choose other licensed anti-virus software such as Kaspersky as per organizational needs and user feedback.

3. All cookies shall generally be disabled. Cookies can pass on personal access credentials such as user ID and passwords which can be detrimental to the organization. However, specific applications may require cookies and users may enable cookies on a case to case basis. In case of any confusion users should seek guidance of the IS Unit.

4. If an employee is unsure about what constitutes acceptable Internet usage then he/she may ask the IS Unit for guidance and clarification.

5. Any user violating these policies can be denied internet access temporarily and may be subject to disciplinary actions where appropriate.

(G)   Use of Email Systems:

Overview:

e-Mail has become the primary medium of communication today. All employees need to have email addresses assigned by the organization. However, most employees also have personal email addresses from webmail services such as Google Mail, Yahoo Mail, Hotmail and others. There needs to be some discipline in the use of official and personal email addresses.

Recommendation:

1. The use of organizational e-mail system shall be restricted to official purposes only.
2. Incidental personal use is permissible if such use does not interfere with employee productivity, does not preempt any business activity and does not consume more than a trivial amount of organizational resources.
3. Users shall refrain from sending e-mail messages that may be considered lewd, offensive or harassing by or to other people.
4. Users shall check e-mails at least twice daily – at the beginning and end of work each day. However, checking emails once an hour is recommended.
5. Users shall delete unsolicited messages and attachments that are not needed for any official business. However, all official messages are to be left intact at all times.

Adoption:

1. IS Unit shall assign permanent email addresses to all Users which shall be based on a consistent concatenation rule such as "initials of first two names plus last name; in case of duplicate email IDs assign a serial number at the end; example: *Md. Azizur Rahman's* email address will be marahman@lged.gov.bd while *Md. Abdur Rahman's* email address will be marahman2@lged.gov.bd. Such mail addresses shall be assigned by the IS Unit when the Admin department notifies IS of any new employees joining LGED at any time. At the end of the employment tenure, whether contractual or regular, the email address shall be deactivated.
2. The above official email addressing system, in line global best practices, requires Active Directory services which are not yet in practice at LGED. Until AD services are fully operational LGED may continue its current practice of assigning email addresses based on designations such as ACE.PL@LGED.GOV.BD.
3. IS Unit shall maintain a backup of all official mailboxes at the Data Center.
4. Personal email addresses may be used as alternate official email addresses. However, in that case the User shall notify the IS Unit about the personal email address(es) to be used as alternate email addresses for official business. IS Unit will record such personal email addresses in the profile of the employee in the PIMS application.
5. Mail attachments need to be under a certain size. Users may check with IS Unit on the prevailing attachment size restrictions.
6. Users are advised to use a signature block at the bottom of electronic mail messages. Signature blocks should be short, preferably not more than six

lines, and should include the user's name, electronic mail address, and postal address; a phone number is optional.

7. Users need to be aware, that unless encrypted, electronic mail is not strictly private communication, because others may be able to read or access such mails. Electronic mail may best be treated as if it is a postcard rather than a sealed letter.

(H)   Use of External Media:

Overview:

Use of external media is usually the easiest means to transfer or store information. These days pen-drives (USB-drives) are frequently used for transporting data from place to place. Other external media include CD/DVD and USB hard drives. Though very useful external media are most often carriers of harmful virus and malware.

Recommendation:

1. Use of all external devices like pen-drives and CDs should be discouraged; exchange of data should be done over the network as much as possible. Remote access media such as VPNs or modems should be turned off when not in use.
2. The anti-virus software should be configured to automatically scan all inbound data, either from the network or from external media, for viruses and malware. When prompted to scan an external media such as a pen-drive, always choose scan (never skip this step; skipping a scan may save a minute but will kill hours and cause agonizing days if a virus catches on).

Adoption:

The LGED handles a lot of data in its operations. As a publicly funded institution, it is particularly important that all such data must be properly handled by all staff members of the organization. Any unauthorized disclosure or leakage of such data is not only against the interest of the organization but also the public.

1. Storage of official data on external media shall be controlled and restricted. Always scan external media for virus before transferring any data.
2. Devices such as USB drives, mobile phones and computer pads/tablets are risky places to store data, as they are small and easily lost or stolen.

3. Never trust an external media from any source. Always scan such devices for virus before use. Detach the external media immediately after use.

(I)   Use of Hardcopy:

Overview:

Today's information and communication technologies provide many opportunities for businesses to function with far less paper. Electronic mail, Intranets, Internet and document scanners can radically reduce paper use, while also saving time and money.

Recommendation:

There are many easy ways for businesses and organizations to reduce their paper use and costs. Here are practical tips to help LGED implement a cost-saving, paper reduction program:

1. It is simply too easy to push the print-button. For example, much paper is wasted by printing out single line emails or printing out unnecessary copies of documents.
2. Departments should carefully assess their needs before ordering bulk print copies of information materials, like annual reports or brochures. In many cases hundreds if not thousands of un-used copies end up in storage rooms clogging up storage space.
3. Think twice if you really need to print – if it is necessary to print make sure you print on both sides (duplex). This is a really easy way to reduce paper consumption by half.
4. When you hold a meeting, check to see if you really need to have hard copies of preparatory materials available for each participant.
5. Encourage people to use their computers for reviewing documents and note-making.
6. Make sure meeting participants have electronic access to all the materials beforehand – encourage those using computers not to print out copies. If you must supply additional materials at the meeting, consider burning CDs for all participants.
7. Make copies "as needed" rather than in large batches at one time. Frequently, extra copies of important internal documents become outdated quickly and only end up being discarded. Making copies "as needed" can reduce this problem significantly.
8. Use electronic means to communicate with customers, for press release/media relations.

9. Use e-mail instead of memos and faxes for inter-office memos, announcing meetings, and targeted communications. Use group e-mail lists to "broadcast" important messages efficiently and inexpensively.
10. For editing and reviewing of larger documents, transfer documents via shared directories at the data center or by e-mail rather than sending a printed copy.
11. Use electronic communications for directories, forms, bulletins, manuals, reports, and storage when possible (don't print them unless absolutely necessary).

Adoption:

1. Encourage online leave applications and material requisitions
2. Organize in-house trainings on e-learning platforms
3. Encourage video conferencing over physical meetings
4. Encourage electronic exchange of documents via email or shared directories.

(J)   Request for Services:

Overview:

Service requests on use of information systems and on getting out of difficult situations are quite frequent in any large organization. To address such service requests many organizations have a central point of contact for handling customer, user and other issues. The service desk types are based on the skill level and resolution rates for service calls. The different service desk types include Call center, Contact center, Help desk etc.

Recommendation:

The IS Unit needs to set up a help desk to provide resolution of any service related problems. If anyone faces a problem then he/she can go to or call the help desk which shall be structured into different levels to handle different types of questions. For example, a first-level help may be prepared to answer the questions or provide the information commonly found among the Frequently Asked Questions (FAQ) sheet or in a knowledge base. If the issue is not resolved at the first level, it can be forwarded to a second level with resources to handle more complex issues. LGED may also have a third line of support to deal with software-specific needs, such as updates and bug-fixes that directly affect a specific User. Such multi-level service desks can be very effectively managed via outsourced IT service vendors. An SLA template for IT services is attached as annexure A.

Adoption:

1. Set up a helpdesk operation with 3 service agents initially in two shifts – morning shift from 8am to 3pm and evening shift from 3pm to 10pm during weekdays and 8am to 1pm during weekends. The helpdesk can be outsourced to a IT vendor with appropriate SLA.
2. Provide a room with landline and mobile phones to the helpdesk seats and publish the phone numbers to all Users.
3. Train the helpdesk agents continually on how to support the enterprise-wide applications such as PIMS, uFMS, ePMS, IDSS and others as features and user interface (UI) of applications may change from time to time.

(K) Outsourcing:

Overview:

Contracting outsourced vendors to provide IS services is commonplace these days. Such IS services could be for software development, network operations, software support or various other IS functions. IS outsourcing contract template is attached as annexure C.

Recommendation:

LGED is a civil construction and engineering service delivery organization. It uses IS tools and facilities to augment its capacity to deliver its core services more efficiently and expeditiously. In order to manage its IS resources LGED needs to engage various types of IT outsourcing vendors in the following areas:

1. Helpdesk support services (call and contact center specialists)
2. Custom-built software apps (software development lifecycle specialists)
3. Network operation center services (network administration specialists)
4. IS strategy/operations assessment services (IS capacity development specialists)

Adoption:

1. Identify outsourcing needs in the short, medium and long terms and prepare a plan to engage outsourcing vendors of appropriate tenures.
2. Prepare SLA of all outsourcing engagements.
3. Engage IS personnel not yet in approved organogram under outsourcing arrangements.

(L) SLA (Service Level Agreement):

Overview:

A service-level agreement (SLA) is simply a document describing the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. Usually, SLAs are between organizations and external suppliers, but they may also be between two departments within an organization. Most service providers have standard SLAs — sometimes several, reflecting various levels of service at different prices — that can be a good starting point for negotiation. Two SLA templates are included in this document as guidance.

(M) E-WASTE DISPOSAL POLICY:

E-WASTE (UNUSABLE IT EQUIPMENT) DISPOSAL POLICY OF LGED

1. INTRODUCTION

Electronic waste, also known as e-waste, is the accumulation of electronic products, such as IT equipment, that have outlived their usefulness and needs to be disposed off. These products have toxic components like lead, mercury and cadmium. Improper disposal of e-waste pollutes the environment with hazardous toxins, thereby causing widespread health problems and environmental degradation. With the increase of e-waste generation and the consequent threat of environmental degradation, there is a need for appropriate policy to mitigate hazards from e-waste disposal. Thus proper disposal of IT equipment is both environmentally responsible and often required by law.

In addition, hard drives, USB drives, CD-ROMs and other storage media contain all kinds of official and personal data, some of which could be considered sensitive. In order to protect constituents' data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

LGED utilizes a wide range of IT products, which results in e-waste continually as the IT products become obsolete and/or broken beyond salvage.

Establishment of e-waste management infrastructure, awareness and education, human resource development, and resource mobilization are some of the key strategies encompassed in this policy document.

2. PRINCIPLES OF IT EQUIPMENT DISPOSAL POLICY

The guiding principles are:

I. Environmental Conservation – the organization must endeavor to ensure environmental conservation and protection from the effects of e-waste.
II. Safe Disposal – the organization must recognize the need to dispose of e-waste in a manner that is safe and secure with respect to its staff, organizational operations and its stakeholders.
III. Public Awareness – the organization must acknowledge the importance of an informed society in the sustainable management of e-waste.
IV. Policy Framework – the organization must acknowledge the need to establish clear guidelines on e-waste management.

3. OBJECTIVES OF THE POLICY

The purpose of this policy it to define the guidelines for the disposal of IT equipment and components owned and operated by LGED. Through adopting this policy, LGED seeks to meet the following objectives:
I. To minimize IT-waste generation.
II. To mobilize and sensitize stakeholders on the proper management and handling of IT-waste on a sustainable basis.
III. To develop and implement a critical human resource base knowledgeable in handling IT-waste.
IV. To develop environmentally beneficial IT-waste recycling.
V. To provide guidance on the standards of IT equipment procured by LGED with an eye on e-waste recycling and disposal.

4. SCOPE OF THE POLICY

This policy applies to LGED headquarters and all other zonal and field offices located across Bangladesh. IT equipment and/or peripheral devices that are no longer needed including, but not limited to, the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), monitors, printers, scanners, UPS, network devices, cables, compact and floppy discs, portable storage devices (i.e., USB drives), backup

tapes, printed materials, and any other materials required for IT system functioning but which have reached the end of their useful service life.

5. PROCEDURES

I. Segregate computer monitors, CPUs, peripherals, and other electronic equipment from other wastes/materials. All CPU hard drives must be cleansed as per data sanitization instructions provided by IT unit of LGED prior to offering the material for recycling

II. LGED IT unit requires that all data bearing devices are clearly marked with a notification that all hard drives have been cleansed or removed, as per the Data Sanitization instructions.

III. Store equipment in a manner that prevents damage to such materials while awaiting disposal

IV. Monitors should be stored in an upright position or in a manner that prevents breakage of the screen.

V. Computer monitor power cables should be wrapped up or properly secured before offering it for recycling.

VI. Toner cartridges and paper should be removed from printers prior to disposal.

VII. Departments replacing large equipment, such as large printers or copiers, should reach out attempt to dispose of such equipment with the vendor providing replacement equipment.

VIII. Departments must ensure that leased equipment is returned to the leasing vendor.

IX. Facilities may be contacted to remove electronic waste from LGED owned or maintained spaces that they may provide services.

X. Disposal Committee should be contacted for removal and disposal of e-waste for departments with a large volume of electronic waste.

XI. Disposal Committee will schedule the disposal of electronic waste from all campuses.

XII. Electronic waste disposal may be performed by approved LGED vendors. LGED will maintain all records of disposal, including shipping papers and certificates of recycling where applicable.

6. COMPONENTS OF THE POLICY

This policy covers and is informed by the following components:

A) IT Equipment Disposal

I. When IT assets have reached the end of their useful life they should be sent to the **IT Equipment Disposal Office** for proper disposal.

II. The **IT Equipment Disposal Office** will securely erase all storage mediums in accordance with current industry best practices.

III.   All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting organizational standards.

IV.   No computer or IT equipment may be sold to any individual or outside agency other than through the processes identified in this policy.

V.   No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around LGED. These can be used to dispose of equipment. The **IT Equipment Disposal Office** will properly remove all data prior to final disposal.

VI.   All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

VII.   IT Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

VIII.   The **IT Equipment Disposal Office** will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.

IX.   IT equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

X.   Employee purchase or outside sale of disposed of equipment shall only be allowed after data wiping has been done as described in item V and VI above.

XI.   Equipment which are working, but have reached the end of their useful life for LGED will be made available for purchase by employees.

XII.   A lottery system will be used to determine who has the opportunity to purchase available equipment.

XIII.   All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or "reserve" a system. This ensures that all employees have an equal chance of obtaining disposed of IT equipment.

XIV. Finance and Information Technology departments will determine an appropriate cost for each item.

XV. All purchases are final. No warranty or support will be provided for any equipment sold.

XVI. Any equipment not in working order or remaining after the lottery process will be donated or disposed of according to current environmental guidelines.

XVII. LGED may have contracts with several organizations for donation or proper disposal of outdated technology assets.

XVIII. Prior to leaving LGED premises all equipment must be removed from the Information Technology inventory system.

B) **Legal Framework:** The e-waste or IT-waste policy is underpinned by the environmental laws of Bangladesh.

C) **Capacity Building:** The IT-waste management activities shall be strengthened through capacity building. The existing skills in the area of IT-waste management are limited, yet these skills are a prerequisite for successful protection against IT-waste hazards to the environment and human health. With this LGED shall;
   I. Facilitate development of IT-waste management training modules to cover technical maintenance, dismantling, and sustainable IT-waste management, to provide for environmental and human health benefits.
   II. Develop e-waste business models that will yield social benefits.

D) **Environmentally sound management of IT-waste:** Environmentally sound recycling refers to recycling without causing adverse impact on environment and health. The use of environmentally sound technology needs to be encouraged in order to increase efficiency of the processes, maximize recovery of materials, conserve energy and reduce waste generation to a minimum. This policy shall be shared with all stakeholders and seek their accountability regarding e-waste. LGED shall achieve environmentally sound e-waste management through the following measures:
   I. Recycling IT-waste in authorized/centralized areas.
   II. Sourcing appropriate technologies for recycling.
   III. Ensuring use of environmentally sound technologies to maximize recovery and minimize waste generation.
   IV. Encouraging training and skills development for environmentally safe handling of IT-waste.

E) **Awareness and Information Dissemination:** There is extremely low awareness on hazards of e-waste among the people of Bangladesh. There is also limited awareness regarding the detrimental effects of e-waste among the staff of LGED. Awareness campaigns on how to handle IT-waste are non-existent. Awareness needs to be created among all stakeholders in the IT-waste value chain. Training and awareness events need to be organized involving other stakeholders. To this end, LGED shall:

I. Develop a strategy for education efforts regarding e-waste management and handling.
II. Develop a web portal for e-waste management and handling related resources.
III. Organize events to promote IT-waste awareness.

F) **Resource Mobilization:** LGED shall provide resources for IT-waste management as follows:

I. Increase the budgetary allocation for reducing IT-waste related risks.
II. Put in place mechanism for resource mobilization from development partners.
III. Provide the equipments, devices and other support systems for effective and efficient management and handling of IT-waste.

7. POLICY COMPLIANCE

A) **Compliance Measurement:** IT Equipment Disposal Office will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

B) **Exceptions:** Any exception to the policy must be approved by the IT Equipment Disposal Office in advance.

C) **Non-Compliance:** An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8. E-WASTE POLICY IMPLEMENTATION PLAN

The **IT Equipment Disposal Office** of LGED shall

I. Liaise with all offices/departments/sections and will identify IT-waste
II. Ensure that IT-waste is collected every quarter and kept in an appropriate storage pending approval of the disposal committee
III. Profile all IT-waste generated at least once every quarter and prepare a report to the disposal committee with recommendations for disposal

IV. Execute the recommendations of the disposal committee and prepare a report to the management of LGED
V. Organize quarterly awareness forums for sensitization of LGED staff on IT-waste
VI. Organize programs quarterly for voluntary surrender of IT-waste at different locations across the country

9. E-WASTE ADVISORY COMMITTEE

LGED shall constitute an IT-waste advisory committee that shall:

I. Oversee implementation of this policy
II. Develop procedures and administer instructions for collection, sorting, disassembly, packaging, storage and disposal of IT-waste
III. Minimize the unintended consequences of IT-waste handling
IV. Provide flexibility to adopt the required changes time to time
V. Review inputs from all stakeholders
VI. Monitor implementation of this policy and advise LGED management as appropriate
VII. Review this policy from time to time and advise on improvement of the policy

10.   MONITORING AND EVALUATION

Realization of the output of this policy shall require consistent monitoring and evaluation of the output indicators. A monitoring and evaluation framework will be established for midterm review of this policy.

The policy implementation shall be reviewed through the performance contracting execution and reporting structures. A policy implementation shall be developed every financial year including actions, actors, time and resource plans.

11.   MANDATORY REVIEW OF E-WASTE DISPOSAL POLICY

The policy shall be reviewed every five (5) years or as needed.

12.   REVISION HISTORY

Date of Change	Responsible	Summary of Changes

ANNEXURE – A

Template I
For
IT Support & Services-SLA

Service Level Agreement (SLA) for IT Support & Services

Technohaven – IBCS Primax Consortium

1 INTRODUCTION

1.1 This Service Level Agreement (SLA) defines the levels of service to be delivered by the <VENDOR> to the customers Headquarters and associated business units.

1.2 IS Service Delivery within <VENDOR> is managed and reviewed in accordance with the IT Infrastructure Library (ITIL) set of practices for IS Service Management. ITIL is the industry best practice model derived from the collective experiences of technical support providers worldwide since 1989.

2 <VENDOR> RESPONSIBILITIES

HQ <VENDOR> is responsible for providing the following to customers to enable IS Service Management within the targets set in this SLA.

2.1 SERVICE DESK

2.1.1 A Service desk service will be provided as a standardized means of reporting and tracking IS incidents, service requests and procurements. Details of jobs will be provided to the customer by means of regular reports and also online access via a self service portal. Regular reports will be produced to show actual performance against the SLA targets.

2.1.2 All procurement requests for all customers will be processed and tracked via the Service desk in line with the policy at Annex A. All requests for procurement should be submitted to the Service desk via the One Page Business Case (OPBC) form at Annex B

2.1.3 A random 5 % sample of completed tasks will generate a request to submit a customer feedback survey. The requester will be asked to rate the speed and efficiency with which the specific job was handled and also invited to comment on their overall level of satisfaction with the <VENDOR>.

2.1.4 The <VENDOR> will make a Self Service Portal available to customers to facilitate online tracking of requests, to access self help solutions and to view and share best practice.

2.2 INCIDENT MANAGEMENT

2.2.1 All calls to the Service Desk will be recorded on a call logging system with a unique number allocated to each incident for tracking purposes.

2.2.2 The <VENDOR> aims to resolve each reported incident in the shortest time possible so that the affected service can be resumed as soon as possible. Wherever possible the Service desk will implement a "first time fix" e.g. automated password resets. Consideration will be given to introducing "first time fix" KPI targets into subsequent reviews of this SLA.

2.2.3 When additional information is required from the customer to allow investigation or resolution of the fault (e.g. asset tag number) the <VENDOR> may mark the call as "awaiting customer response". The elapsed time of that particular incident will remain on hold until the required information is provided. If no response to a request for

additional information is received for 3 working days the Service desk will close the call. Should the customer wish to re-open the call the call by providing the requested information they can do this at any time.

2.3   SOFTWARE RELEASE MANAGEMENT

2.3.1   Software release management is the process of testing and integrating software required by the customer and making it available for deployment wherever required.

2.3.2   Software approved for release will be added to the <VENDOR> Software Catalogue.

2.4   REPAIR AND REPLACEMENT OF FAULTY EQUIPMENT

2.4.1   The <VENDOR> will repair and replace all equipment that is faulty or has become damaged through normal day to day use. The <VENDOR> will ensure that appropriate resources to repair equipment are maintained, where appropriate via underpinning contracts.

2.5   INSTALLATION OF NEW EQUIPMENT

2.5.1   The <VENDOR> is responsible for installing all new equipment procured through the procedures laid out in this SLA onto the networks.

2.6   AGREE RESPONSE TIMES VIA SERVICE LEVEL REVIEWS

2.6.1   Service level management is the process of ensuring that IS services are supported to an acceptable level. It involves understanding the IS requirements of the customer and working within the constraints of available resources. Effective service review will result in an agreed, consistent level of service that is aligned with available resources. This will facilitate an environment where continual service improvement can be implemented and monitored through service improvement plans.

2.6.2   The <VENDOR> will take part in Service Level review meetings providing statistics on incidents and projects undertaken. Any changes to this SLA will be promulgated and agreed via the SLR process.

2.7   SUPPORT BUSINESS CONTINUITY AND DISASTER RECOVERY

2.7.1   The <VENDOR> is responsible for ensuring that systems and data are suitably backed up and secure to support customers' own Business Continuity and Disaster Recovery Plans.

2.8   MANAGE THE ASSET CONFIGURATION

2.8.1   Configuration Management is the process of creating and maintaining an up-to-date record of all components of the IS infrastructure.

2.8.2   The <VENDOR> will provide asset monitoring and tracking of all IS assets. All assets will be recorded by HQ <VENDOR> on the asset database. Extracts from this asset database will be provided to individual s annually to assist the annual asset verification exercise.

2.8.3   The <VENDOR> will be responsible for the removal, de-commissioning and disposal of all redundant IS equipment in accordance with extant MOD policy.

3   CUSTOMER RESPONSIBILITIES

<VENDOR> s and other customers of the IS Service are responsible for the following to IS Service Management to be delivered within the targets set in this SLA.

3.1   AGREE SERVICE RESPONSE TIMES VIA SERVICE LEVEL REVIEW

3.1.1   The customer will assist with the Service Level Review and Service Improvement Planning processes by attending regular Service Level review meetings.

3.2   REPORT FAULTS AND SERVICE REQUESTS THROUGH THE AGREED PROCEDURES

3.2.1   The customer will report all faults and enquiries via the Service desk in accordance with the procedures at Section 4.

3.3   ALLOW ACCESS TO PREMISES AND SYSTEMS

3.3.1   Allow appropriate access at all reasonable times to rooms and equipment to enable <VENDOR> IS staff and authorized sub-contractors to make changes necessary to provide the required level of service.
.

3.4   TAKE CARE OF EQUIPMENT

3.4.1   Take all reasonable care of IS equipment and not damage, tamper with or make any attempt to repair the installed equipment

3.4.2   Take all reasonable steps to prevent unauthorized access to installations, ducting etc. that could compromise the integrity of the equipment or communication system. It should be noted that attempted repairs by unauthorized personnel can invalidate support cover and manufacturer's warranty. It should also be noted that the costs of repairing damage which has been caused by misuse of the equipment or that is deemed not fair wear and tear will fall to the customer rather than to the

<VENDOR>.

3.4.3   Individual s will be responsible for reporting to the Police any loss of IS equipment assigned to them, whether it has been stolen in the possession of an employee whilst they were in a different location. The process for writing-off and replacing IS equipment cannot be triggered until the POLICE Report is received by the Service desk.

3.5   MAINTAIN LOCAL IS ASSET REGISTER

3.5.1   Maintain an asset register of all MoD equipment issued and to submit this to the <VENDOR> annually on request.

3.6   ORDER AND FUND APPROPRIATE WORKS SERVICES

3.6.1   Take the necessary action to order and fund the works services required to support the IS installed. This includes electrical supplies and air conditioning to the room where the main server cabinet is located to allow the equipment housed therein to operate within its contractual temperature parameters.

3.7   APPOINT A LOCAL MEMBER OF STAFF TO CARRY OUT APPROPRIATE IS TASKS

3.7.1   Each should appoint or nominate a local member of staff to carry out appropriate IS support tasks and to act as the focal point for day to day communication with the <VENDOR>.

3.7.2   The scope and level of incidents that can be dealt with and allocated to this member of staff will be discussed and reviewed at SLR meetings. The relationship between the <VENDOR> and the IS point of contact is a crucial element in allowing the targets within this SLA to be met. This is particularly pertinent in RoW settings where time zone differences impact on the availability of centrally located support staff during office hours.

4   FAULT REPORTING & SERVICEDESK PROCEDURES

4.1   OUTLINE OF PROCESSES

4.1.1   When a problem occurs users should not contact their IS Technical Support Officer directly, instead the following call-logging procedures should be followed. Contact should be made with the IS Service Desk via e-mail or by telephone, as follows:

- e-mail: ict.helpdesk.hq@ServiceProvider.com

- Service Desk <Telephone Number>

    Note: The preferred method is by e-mail. The Service Desk email system is operational 24 hours a day for the reporting of incidents and service requests.

The Service Desk will:

a. Answer and process all reported incidents promptly and in a professional manner.

b. Ask the caller to supply the following information when a problem is logged:

- Contact name, number and department/.
- Location of asset
- A full description of the fault and history of any remedial action already attempted
- <VENDOR> Asset TAG number

Note: The following information may also be requested, if applicable:
- Contact name and number of the affected user if different from the person logging the call.
- Make and model of equipment
- 7 Digit Service TAG Number or Serial Number

c. Allocate a Call Reference Number for all reported incidents and pass them to the appropriate support staff for action. The Call Reference Number will be notified to the customer by email. The customer should note this reference number and quote it when making enquiries about the status of outstanding calls.

d. Periodically advise the customer of the progress of an incident where resolution is likely to exceed the SLA response times, advice the customer of the escalation action being taken and likely time of restoration of service.

e. Always advice the customer when equipment or systems have been returned to service or when the call has been closed.

f. Treat all incidents reported as MEDIUM or LOW unless a higher priority level is clearly required as indicated in this SLA or a higher priority is clearly stated and justified within the content of the request.

g. Distribute monthly reports of all Service desk jobs undertaken in each individual. Prepare and distribute reports and statistical analysis of reported incidents on a regular basis to Service Level review Meetings and other relevant parties on request.

4.1.2 The organization's nominated IS member of staff will carry out appropriate IS support tasks within the organization and to act as the focal point for day to day communication with the <VENDOR>.

5 ESCALATION PROCEDURES

5.1 The first point of escalation for any incident, OPBC, or project is to contact the Service desk to request an update on the current state of play. The preferred means of doing this is via an email stating the relevant job number, this will automatically

added to the audit trail of the job in question, as will any responses. If the customer is dissatisfied with the response to this request from the helpdesk for any reason, they should contact the IS Systems Manager at HQ <VENDOR>. This contact can be by any means available, email, phone personal approach etc. It will assist with progressing the escalation request if the customer can quote the Service desk job number, their reason for escalation, and their desired outcome.

5.2   Complaints Procedure – more content to follow

6   DESCRIPTION OF SERVICE LEVELS AND TARGETS

6.1   It is generally difficult to provide accurate resolution time of individual incidents until the nature of the fault has been fully investigated. However, each and every reported incident will be resolved in the shortest possible time and with the least disruption to the customer that resources will allow. In some cases a temporary work around may be put in place to alleviate the symptoms while the underlying causes are further investigated via root cause analysis.

6.2   The SLA target times for each reported call will be allocated a target resolution time in line with the following table.

Item	PERFORMANCE INDICATORS	TARGETS
Service time coverage	For the purposes of this SLA one working day equates to 09:00 to 17:00 BDT i.e. the time zone of the Service desk Software Server	
Critical Incidents – Complete network failure, loss of core service (e.g. Server Failure)	Initial response within 1 working day – resolved within 2 working days	90 % of incidents
Severity High – Incidents that affect the partial loss of a core service, such as the loss of Internet connection or network problem affecting > 20 users - loss of central Printing facility. An incident that affects the loss of a critical business application, e.g. Integris or Target Tracker	Initial response within 2 working days – resolved within 3 working days	90 % of incidents
Severity Medium - incidents that affect the productivity of the individual customer in respect of a single PC, Laptop, Printer, Interactive Whiteboard, Digital Projector. The majority of incidents will fall into this category	Initial response within 3 working days – resolved within 6 working days	80 % of incidents

Template I – IT Support Services SLA

Item	PERFORMANCE INDICATORS	TARGETS
Severity Low – Routine work requests, e.g. client software installations of approved packages, PC client moves, printer moves and printer Installs.	Initial response within 10 working days – resolved within 15 working days	90 % of incidents
All Project related work, e.g. server moves and installations, major changes, major software releases, multiple client moves.	Subject to OPBC - Minor projects to be progressed and monitored via Service desk and SLR meetings Major Projects to be reviewed	Specific targets for each project set during project approval and planning
T&I of curriculum software	Software released and (if compatible) installed within 20 working days of receipt of media and licenses for T&I	95 % of submissions
Purchases of equipment **NB** The procurement processes is due to be segregated in the near future. This will allow metrics to be recorded on the times taken for each constituent part of the process from initial request to receipt of goods. Additional KPIs will be introduced and agreed in line with discussions at Service Level review Meetings.	Orders placed within 30 days of approval of OPBC	100% of OPBCs
User Satisfaction Surveys	All submitted user satisfaction surveys with a total score of < 50% will be investigated by IS Systems Manager	A random 5 % of Service desk calls receive a request to submit a satisfaction survey

OPBC – One Page Business Case

7   REPORTING AND SERVICE REVIEW

7.1   This SLA is subject to continual review via the process of Service Level Review. The Terms of Reference for SLR meetings can be found at Annex C.

7.2   The <VENDOR> will be responsible for compiling performance reports for presentation to SLR meetings and other parties as required.

ANNEX 1 – IS PROCUREMENT POLICY FOR <VENDOR>

1.   CORE INFRASTRUCTURE

A core set of infrastructure has been agreed for all <VENDOR s> as set out in this SLA. The core infrastructure may be supplemented using delegated IS funding in accordance with the following guidelines.

Please note that it is a responsibility to fund the technical refresh of any items purchased using delegated IS funding.

Please also note that if the IS Technical Support Officer or the IS Service desk are not consulted prior to procurement action being taken, the organization is taking a risk that the Hardware/Software cannot be connected to or loaded onto the IS infrastructure.

IS HARDWARE

Defined as: Computers, Monitors, Laptops, PDAs, iPods, Network printers, Projectors, Wireless Access Points, Switches, Plasma touch screens, SMART tables and Interactive Whiteboards.

All the above items may be acquired using delegated IS funding; however they are to be approved by the IS Unit and authorized via the OPBC process. The OPBC form at Annex B should be submitted to ict.helpdesk.hq@<VENDOR>.com with the necessary budgetary approval.

2.   IS SOFTWARE

Defined as: Any software programme run from or downloaded from a CD-ROM or downloaded from the Internet whose software is permanently resident on the hard disk of a PC

- It is **strongly recommended** that curriculum software should not be purchased by s without first consulting the <VENDOR> Approved Software Catalogue to see whether a similar package is already available. If not, s should approach their IS Technical Support Officer to seek:

  - ➤ Advice on compatibility of the software with the s operating systems
  - ➤ A best price based on <VENDOR> -wide bulk buys

- The software contained on the catalogue has already passed the T& I process so will be made available more quickly. This software will also be familiar for employees who may have encountered the same software in other <VENDOR> s
- If a suitable software title can not be found on the catalogue customers should consult with their local IS Tech Support Officer or contact the Service desk for further guidance. It is recommended that an evaluation copy of new software is acquired before committing any expenditure. This evaluation copy should be submitted to the service desk for T&I. This will ensure that :

  - ➤ Compatibility issues of the software with the s operating systems will be considered before purchase
    - ➤ Software will not be purchased that is already covered by an <VENDOR> wide license
    - ➤ The software will be fully supported
    - ➤ <VENDOR> can obtain the best value for money on bulk buys

- Software which has not been purchased and tested through the above process will not be installed onto <VENDOR> systems and is not covered under the terms of this Service Level Agreement.

- MoD rules preclude s from procuring their own software site licenses that contain a maintenance agreement. Additionally it should be noted that Anti-Virus Software, Microsoft Office and Windows 2003 licenses are purchased centrally by HQ <VENDOR> .

- The target time for the test and integration of new software into these releases is shown at Section 6.

3.   IS PERIPHERALS

Defined as: TVs, display screens, Sound Systems, Apple TVs, DVD Recorder/Players, Digital Cameras/Camcorders, Scanners or any other plug and play devices.

All the above items may be purchased by using delegated IS funding. However it is **strongly recommended** that the above peripherals are not purchased by s, without first approaching your IS Technical Support Officer or the Service desk to seek advice on compatibility of the chosen models with the systems.

4.   IS CONSUMABLES

Defined as: Ink Cartridges for Printers or Facsimile Machines, Projector Bulbs.

All the above items can be purchased by s using delegated funding. MOD enabling contracts must be used, unless a cheaper source is identified.

ANNEX 2 – ONE PAGE BUSINESS CASE (OPBC)

ANNEX B TO <VENDOR> IS SLA

HQ <VENDOR> IS UNIT
E-mail: ict.helpdesk.hq@<VENDOR>.com
Helpdesk Tel – Mil: 94881 3547   Civ: +49(0)5219 254 3547

ONE PAGE BUSINESS CASE

1. END USER POC ADDRESS:	**NAME:** **APPOINTMENT:** **TEL NO:** **E-MAIL:**
2. WHAT	
3. WHY	
4. WHO	
5. WHERE	
6. WHEN	
7. FUNDING	UIN: RAC: BEX000
8. AUTHORITY	
9. AREA TECHNICAL SUPPORT OFFICERS COMMENTS	
. 10. DETAILS FOR DELIVERY	

APPENDIX 1 TO ANNEX B TO <VENDOR> IS SLA
GUIDANCE FOR COMPLETION – ONE PAGE BUSINESS CASE

1. END USER POC	**NAME:** *The name of the person who all queries regarding the Submission should be directed to.* **APPOINTMENT:** **ADDRESS:** **TEL NO:** *(Civilian **AND** Military Tel No's to be provided where applicable).* **E-MAIL:** *(Only xxx@<VENDOR>.com or xxx@mod.uk e-mail addresses accepted. Any requests sent from non-official e-mail addresses will be deleted.)*
2. WHAT	*This is where you describe the requirement. You should identify the functionality you require. Do not specify particular models of equipment (unless essential to the requirement) as equipment is bought to a <VENDOR> agreed standard.*
3. WHY	*What is the rationale? What is the driver? It may be a better way of doing business: a way to save time or money, or it may be a requirement to comply with new legislation. Remember that there are numerous good ideas that would benefit the business, but there is a limited budget. This is where you state the case in detail why your aspiration should be considered. Try to identify key benefits; does this address a deficiency? Does it make the business function better? Will it lead to savings? What benefits will be* *What is the impact of this request not being approved?*
4. WHO	*Identify who will benefit. Indicate the scope.*
5. WHERE	*Where will the equipment be used*
6. WHEN	*Date required. The normal procurement cycle takes time so please be realistic, remembering that requests for small amounts of equipment may be put on hold to wait for other requests of a similar nature in order to make use of any possible discounts for purchasing in larger quantities.*
7. FUNDING	*Do you feel HQ <VENDOR> should pay for the equipment detailed in the* *request? If so, why?* *If the are planning to buy from within their own budget, should the request be approved, you should provide the UIN & RAC number under which the purchase is to be procured.*
8. AUTHORITY	*Under who's authority is this request being submitted.*
9. AREA TECHNICAL	*Does the request fit within the current network model? Are there* *any technical issues which may need investigating? Is there*

SUPPORT OFFICERS COMMENTS	*sufficient network infrastructure to facilitate the request, i.e. Wireless Network coverage, network access points or, power supplies for the equipment?*
10. DETAILS FOR DELIVERY	*Where, and to whom, is the equipment to be delivered?*

ANNEX 3 – SERVICE LEVEL REVIEW TERMS OF REFERENCE

Purpose

The purpose of the IS Service Level Review (SLR) Meeting is to review the level of IS service currently being delivered, to identify areas requiring improvement, and to formulate the IS service improvement plan for review by subsequent SLR meetings.

Objectives

The primary objective is to measure the level of IS Service provision. The secondary objective and a product of holding regular local SLR meetings is to build a joint understanding of ;

- The IS requirements of the s/Business Units involved
- The IS Services delivered to these units
- The processes and procedures and resources which are used to support them
- Local factors, priorities and future plans
- Review progress and plan IS developments for the next period.

Membership

The membership of the SLR will be:

- IS Systems Manager (Chair)
- Consortia Chair
- Head Employees / Head of Business units
- Relevant IS Tech Support Officer

Other staff will be invited as appropriate, e.g.

- IS Config & System Manager
- Consortia Business Manager

Framework agenda

The agenda for a typical SLR meeting would include the following agenda items;

1. Introductions

2. Review of Service Level Agreement

3. Review of performance indicators

4. Technical update

5. Forthcoming local changes

6. Service Improvement objectives and plan

Frequency

The SLR will meet at least twice yearly.

ANNEXURE – B

Template II
For
Outsourcing Services Contract

IT OUTSOURCING SERVICE AGREEMENT

Technohaven – IBCS Primax Consortium

IT OUTSOURCING SERVICE AGREEMENT BETWEEN

_____

AND

_____

THIS AGREEMENT between _____ ("OUTSOURCER") and _____("CLIENT") is made this _____ day of _____, _____.

WHEREAS, the CLIENT desires to purchase IT management and operation outsourcing services in support of the management and operation of the company's Information Technology need ; and

WHEREAS, OUTSOURCER wishes to provide the total outsourcing services described herein in accordance with the terms and conditions hereof;

NOW THEREFORE, in consideration of the payments herein agreed to be made and the covenants and agreement herein contained, the parties hereto, intending to be legally bound, hereby agree to the following:

1. SERVICES

Starting on the Effective Date (as defined in Section 3.1), OUTSOURCER shall perform the IT Outsourcing services described in this Agreement and Exhibit A, attached hereto and made a part hereof ("Scope of Services").

2. COST FOR SERVICES

The costs for services to be provided by OUTSOURCER are set forth in Exhibit B attached hereto and made a part hereof. Such costs shall be subject to a cost of living adjustment.

3. TERMS AND CONDITIONS

3.1 Term:

This Agreement shall commence on _____, 19____ (the "Effective Date"), and terminate on _____, 19____.

3.2 Invoices and Payment Terms:

3.2.1 OUTSOURCER shall submit monthly invoices to the CLIENT. Invoices shall be issued before services are rendered by OUTSOURCER and shall be submitted by OUTSOURCER at least 30 business days before payment is due by the CLIENT.

3.2.2 The monthly amounts to be paid by the CLIENT for OUTSOURCER staff services and expenses. The CLIENT shall pay according to this schedule. Payment not received within [five (5)] days of the due date will be subject to an interest charge. All interest charges will be computed at

the current prime rate.

3.3 Data Processing Equipment and Supplies:

Subject to Section 3.9(c) below, as between the parties, the CLIENT reserves and retains the right, title and interest in any and all computing equipment, software, systems, data, output and other materials or property except that which is furnished by OUTSOURCER and is not developed pursuant to this Agreement, which retains such rights itself. Upon expiration or earlier termination of this Agreement, OUTSOURCER shall relinquish to CLIENT the use of equipment provided by CLIENT in as good condition as when turned over to OUTSOURCER, reasonable wear and tear excepted.

3.3.2 All costs relating to data processing equipment and supplies for the CLIENT's computer functions shall be the responsibility of the CLIENT.

3.3.3 All costs relating to OUTSOURCER's consultants fee, salaries, Medical, Insurance, recruitment fee, training expenses shall be the responsibility of the OUTSOURCER.

3.3.4 The CLIENT shall also provide to OUTSOURCER, at no charge to OUTSOURCER subject to Section 3.17 CLIENT Policy and Procedures, in order to allow OUTSOURCER to perform under this Agreement.

(a) All utilities, including any special power and air conditioning needed, as determined solely by CLIENT, to operate the CLIENT's data processing equipment and storage of computer supplies;

(b) Storage, in an area removed from the data processing site, for historical data and backup material that may be needed to reconstruct data files in the event working files are destroyed by natural disasters, fire, riots or other causes;

(c) Computing supplies such as paper, forms, ribbons, tapes, disk packs and microfilm; and

(d) Security, fire control equipment and janitorial support for the CLIENT's data processing facilities.

3.4 Work Space:

At no charge to OUTSOURCER, subject to Section 3.17 CLIENT Policy and Procedures, the CLIENT shall provide OUTSOURCER, with an appropriately furnished, conveniently located office or other suitable work space for use by the OUTSOURCER staff in performing work under this Agreement. Also at no charge to OUTSOURCER, the CLIENT shall provide office supplies, telephone service and reproduction, telecommunications and office equipment reasonable and necessary to support OUTSOURCER's staff and performance of this Agreement.

3.5 Use of Data Processing Equipment:

At no charge to OUTSOURCER, subject to Section 3.17 CLIENT Policy and Procedures, the CLIENT shall provide OUTSOURCER access to all equipment, equipment services, programs and supplies necessary to support the computing needs of the CLIENT. The CLIENT shall provide
OUTSOURCER's staffs access to all such equipment so that OUTSOURCER may perform its obligations under this Agreement including, but not limited to, operating all such equipment.

3.6 Use of Software and Access to Personnel:

For purposes of performance under this Agreement, OUTSOURCER shall have complete access to, shall operate and shall, subject to CLIENT's approval and obligations of CLIENT under third party agreements, have the right to modify or alter all CLIENT software programs and related material, pursuant to the Scope of Services. OUTSOURCER shall also have reasonable access to the CLIENT's management, professional and operating personnel necessary for performance under this Agreement, as well as to all materials, records, discs, tapes or other information necessary to perform the services contemplated herein. OUTSOURCER and CLIENT each realize that time is of the essence in order to accomplish the objectives of this Agreement, including the Scope of Services. OUTSOURCER agrees to respond to requests for support from CLIENT in a timely and reasonable manner. CLIENT agrees to handle OUTSOURCER's requests for support, to the best of its ability, in a timely and reasonable manner.

3.7 Status Reporting:

OUTSOURCER management staff shall conduct regular meetings with the CLIENT **Contract** Administrator (as defined in Section 4.2.1 hereof) and such other persons as may be designated by the CLIENT to formally review OUTSOURCER performance under the terms of this Agreement. These meetings shall be conducted at a time and location mutually agreed upon.
OUTSOURCER shall also prepare, on a monthly and quarterly basis, as applicable, a written status report which documents past activities and outlines planned activities for the forthcoming month or year.

3.8 Non-Solicitation:

    3.8.1 Beginning on the Effective Date and continuing for a period of one year from the expiration or termination of this Agreement, the CLIENT shall not, without OUTSOURCER's prior written consent (which consent may be withheld at OUTSOURCER's sole discretion), enter into any contract (including, but not limited to, an employment contract, facilities management contract or consulting contract) with (i) any employee or former employee of OUTSOURCER who performed work under this Agreement within two years of such contract (an "OUTSOURCER Employee") or (ii) any person, firm, corporation or enterprise by which

the OUTSOURCER Employee is employed or with which such OUTSOURCER Employee is affiliated (including, but not limited to, as a consultant, shareholder, partner, officer or director) ("OUTSOURCER Employee's New Firm"), whereby the OUTSOURCER Employee or OUTSOURCER Employee's New Firm would provide to the CLIENT all or part of the services provided by OUTSOURCER to the CLIENT under this Agreement.

3.8.2 Beginning on the Effective Date and continuing for a period of one year from the expiration or termination of this Agreement, OUTSOURCER shall not, without CLIENT's prior written consent (which consent may be withheld at CLIENT's sole discretion), enter into any contract (including, but not limited to, an employment contract, facilities management contract, or consulting contract) with (i) CLIENT employee(s), or (ii) any person, firm, corporation or enterprise by which the CLIENT Employee is employed or with which such CLIENT Employee is affiliated (including, but not limited to, as a consultant, shareholder, partner, officer or director) ("CLIENT Employee's New Firm").

3.9 Confidentiality and Ownership of Material:

3.9.1 Subject to paragraph (c) below, ownership of all data, material and documentation originated and prepared for the CLIENT pursuant to this Agreement shall belong exclusively to the CLIENT. Upon termination of the Agreement, all such data, material and documentation shall be returned by OUTSOURCER to the CLIENT.

3.9.2 CLIENT and OUTSOURCER shall treat the other's "Confidential Information" (as defined below) as proprietary. Each of CLIENT an OUTSOURCER shall (i) exercise due care to keep in confidence and not disclose Confidential Information to any individual other than its own employees who have a "need to know" in order to perform the obligations of CLIENT or OUTSOURCER, as applicable, under this Agreement; (ii) not duplicate or publish any Confidential Information; and (iii) use Confidential Information only for the purposes authorized herein. The foregoing obligations shall not apply to Confidential Information if, and only to the extent that, it:
  (a) is or becomes public knowledge through no fault of either of the parties hereto
  (b) was previously known by the recipient;
  (c) is lawfully provided to the recipient without restriction by an independent third party; or
  (d) must be disclosed pursuant to applicable law or regulation; provided, however, that with respect to exception (a), the disclosing party (i.e., the party who is disclosing to a third party information which is confidential to the other party to this Agreement) shall first establish that the full particulars of the Confidential Information are,

in the combination disclosed to the disclosing party, well known or generally used within the industry, not merely that the individual features are in the public domain or available in isolated segments in two or more readily-available public sources; and provided, further that the burden shall be on the disclosing party to prove the applicability of any of exceptions (a), (b), and (c).

3.9.3 For purposes hereof, "Confidential Information" shall mean manufacturing, engineering, software, business, customer, marketing, financial and other non-public information, reports or trade secrets relating to the business of OUTSOURCER or the CLIENT, as applicable, and created or learned by the CLIENT or OUTSOURCER, as applicable, in connection with the performance of this Agreement.

3.9.4.1 All worldwide right, title and interest in Intellectual Property Rights (as defined below) relating to in severable improvements in software and documentation not owned by or licensed to OUTSOURCER, which improvements are made, conceived or developed by OUTSOURCER in the performance of its duties under this Agreement shall vest exclusively in CLIENT. In severable improvements shall mean those improvements that are not applicable to other software.

3.9.4.2 All worldwide right, title and interest in Intellectual Property Rights in, to, or relating to new software, including without limitation, modules, subroutines and stand-alone programs, and related documentation made, conceived or developed by OUTSOURCER in the performance of its duties under this Agreement shall vest exclusively with CLIENT.

3.9.4.3 All worldwide right, title and interest in Intellectual Property Rights in, to, or relating to severable improvements and modifications made, created, conceived or developed by OUTSOURCER in the performance of its duties under this Agreement, to software and related documentation not owned by or licensed to OUTSOURCER, shall vest exclusively in CLIENT. Severable improvements shall mean those improvements having application in and to other software.

3.9.5 "Intellectual Property Rights" shall mean all patents, trade secrets, and copyrights in, covering, and relating to software and documentation made, created, conceived, developed, improved or modified by OUTSOURCER in the performance of its duties under this Agreement.

3.9.6 Notwithstanding the foregoing to the contrary, Software developed under

grants where OUTSOURCER is responsible for all aspects of development shall be done under a specific change of scope, and the ownership of the software so developed shall be governed by the grant provisions, and if there are no ownership requirements under the grant provisions, then the provisions of subparagraph (d) shall apply.

3.9.7 Notwithstanding the foregoing to the contrary, Software developed under grants where OUTSOURCER provides management and coordination services only shall not require a specific change of scope, and the ownership of the software so developed shall be governed by the grant provisions, and if there are no ownership requirements under the grant provisions, then the provisions of subparagraph 3.9.4 shall apply.

3.10 Liability and Warranties:

3.10.1 Subject to its record retention policies, the CLIENT shall maintain Adequate Supporting Material to enable OUTSOURCER to update or regenerate, as necessary, data files, printer outputs and other data. In the event of loss, damage, destruction of any data, service, system or program due to the negligence of OUTSOURCER, OUTSOURCER's liability therefore shall be limited to either the replacement, repair, reconstruction, redevelopment or regeneration, at OUTSOURCER's option, of the lost, damaged, destroyed or inoperable data, service, system or program from the CLIENT's supporting material or otherwise as appropriate in the method deemed, most suitable, by OUTSOURCER for such action. In the event the CLIENT has failed to maintain Adequate Supporting Material, Outsourcer's liability shall be strictly limited to the same costs of replacement, repair, reconstruction, redevelopment or regeneration as if the CLIENT had so maintained adequate supporting material. Adequate Supporting Material is defined for the purposes of this Section as the original source material or data input documents initially provided to OUTSOURCER or replacement source material or data input documents provided to OUTSOURCER from time to time from which OUTSOURCER has obtained and input data in performance of its services hereunder. OUTSOURCER shall not be liable for any damages resulting or arising from CLIENT's failure to perform its obligations hereunder, provided that OUTSOURCER is not responsible for such failure to perform.

3.10.2 To the extent permitted Law, OUTSOURCER shall not be liable, whether contractually or in tort, for any consequential, special or indirect damages arising out of or in connection with this Agreement. To the extent they are beyond the reasonable control of OUTSOURCER, OUTSOURCER shall not be responsible for schedule delays, inaccuracies or other consequences resulting from incorrect CLIENT data, lateness in delivery of CLIENT's data or the failure of CLIENT's equipment or

personnel.

3.10.3 OUTSOURCER agrees to be liable for, defend and indemnify CLIENT against all claims, suits, judgments or damages, including the cost of administrative hearings, court costs and attorneys fees, arising out of the negligent or intentional acts or omissions, or violations of laws or regulations, of or on the part of OUTSOURCER or its agents, officers, subcontractors or employees, in the course of the operation of this Agreement.

3.10.4 Warranties: OUTSOURCER SHALL PERFORM THE SERVICES UNDER THIS
AGREEMENT IN ACCORDANCE WITH STANDARDS OF CARE, SKILL AND DILIGENCE CONSISTENT WITH RECOGNIZED AND PRUDENT INFORMATION TECHNOLOGY PRACTICES, ALL APPLICABLE LAWS AND REGULATIONS, THE SCOPE OF SERVICES, EXHIBITS, DOCUMENTS AND PROCEDURES APPLICABLE TO THE SERVICES, AND THE DEGREE OF KNOWLEDGE, SKILL AND JUDGEMENT NORMALLY EXERCISED BY PROFESSIONALS WITH RESPECT TO SERVICES OF THE SAME OR SIMILAR NATURE. THIS IS THE ONLY WARRANTY MADE BY OUTSOURCER WITH RESPECT TO ITS SERVICES UNDER THIS AGREEMENT AND TO THE EXTENT PERMITTED BY LAWS IS IN LIEU OF ALL OTHER UNDERSTANDINGS AND ALL WARRANTIES, EXPRESSED, IMPLIED OR STATUTORY, AS TO THE SERVICES TO BE PROVIDED BY OUTSOURCER, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR USE FOR A PARTICULAR PURPOSE.

3.11 Taxes:

This Agreement does not include charges for any taxes, which now or in the future may be deemed by a taxing authority to be applicable to the services to be provided by OUTSOURCER. In the event a taxing authority determines now or in the future that such services are subject to tax,
OUTSOURCER shall invoice such taxes to the CLIENT and the CLIENT shall pay same simultaneously with the payment to which taxes relate.
CLIENT hereby represents that it is not currently subject to any such taxes and will notify OUTSOURCER in a timely manner if CLIENT becomes subject to any such tax. At the time of execution of this Agreement taxes on services provided by OUTSOURCER to CLIENT hereunder are not required to be paid, but if in the future are required, then CLIENT shall pay such taxes.

3.12 Force Majeure:

If either OUTSOURCER or the CLIENT is prevented from performing any task hereunder, in whole or in part, as a result of a cause beyond its reasonable control, which may include an Act of God, war, civil disturbance or organized labor dispute, such failure to perform shall not be grounds for termination of this Agreement.

3.13 Termination:

3.13.1 This Agreement may be terminated by a party (the "Terminating Party") prior to the expiration of its stated term upon the occurrence of an "Event of Default" affecting the other party (the "Terminated Party")

3.13.2 An "Event of Default" shall mean:

(a) failure by a party to timely perform any obligation under this Agreement, including without limitation CLIENT's failure to pay or cause to be paid any sums due in the manner provided in this Agreement within fifteen (15) business days of the date such payments were due; or OUTSOURCER not performing any of its obligations in accordance with this Agreement and all Exhibits thereto; or

(b) any representation or warranty made by either party herein or in any document executed simultaneously and in connection herewith, or in any document or certificate furnished in connection herewith or therewith or pursuant hereto or thereto shall have been incorrect in any material respect at the time made; or

(c) Upon the occurrence of an Event of Default the Terminating Party may give notice of termination to the Terminated Party, identifying in reasonable detail the nature of the Event of Default. Thereupon, the Terminated party shall have 30 days to correct in all material respects the Event of Default (15 business days if the Event of Default consists of CLIENT's failure to pay outstanding sums within 15 business days of the date the payment was due). If the Terminated party so cures the Event of Default, then the notice of termination shall be ineffective. If the Terminated party does not so cure the Event of Default within the aforementioned period, then this Agreement shall be terminated upon the expiration of such period (the "Termination Date").

3.13.3 CLIENT shall pay OUTSOURCER in full, within 15 business days of receipt of a final invoice from OUTSOURCER, for all services rendered up to and including the Termination Date.

3.14 Phase Over:

3.14.1 Prior to the expiration pursuant to its term of this Agreement, OUTSOURCER shall develop a plan for the orderly transition of all services provided by OUTSOURCER under this Agreement (the "Transition Plan"). Such Transition Plan shall be developed by OUTSOURCER in conjunction with OUTSOURCER's employees on site,

the CLIENT's executives and administrators and such other persons as shall be designated by the CLIENT. The CLIENT shall fully cooperate with OUTSOURCER in order to develop the Transition Plan. The Transition Plan shall be completed no later than 90 days prior to expiration of this Agreement. It shall cover, inter alia, the training of CLIENT's personnel in the operation and maintenance of the systems used and operated by OUTSOURCER during the term of the Agreement. CLIENT shall notify OUTSOURCER of its acceptance of the Transition Plan within 14 days of receipt from OUTSOURCER.

3.14.2 OUTSOURCER shall complete all transition activities associated with the orderly termination of this Agreement on or before the date the notice of termination becomes effective. OUTSOURCER shall effect the transition to the CLIENT.

3.14.3 If due to OUTSOURCER's actions or omissions (i) the Transition Plan is not completed within the aforementioned period and the notice of termination becomes effective, or (ii) if the Transition Plan is completed and the notice of termination becomes effective but an orderly transition is not effected prior to the Termination Date, then OUTSOURCER shall continue to perform such services as may be required by the CLIENT, at no additional cost to CLIENT, in order to operate the CLIENT's computing system until such time as an orderly transition may be effected, but no later than 90 days after the Termination Date.

3.14.4 In the event of termination of this Agreement following the occurrence of an Event of Default on the part of OUTSOURCER, OUTSOURCER shall immediately upon the issuance of the notice of termination develop a Transition plan in accordance with the procedures set forth in paragraph (a) except, however, that the Transition Plan shall be completed no later than 30 days after the date of the notice of termination. CLIENT shall notify OUTSOURCER of its acceptance of the Transition Plan within 14 days of receipt from OUTSOURCER. OUTSOURCER shall complete all Transition activities associated with the termination by reason of its default no later than 60 days following OUTSOURCER's receipt of CLIENT's acceptance of the Transition Plan.

3.14.5 In the event of termination of this Agreement following the occurrence of an Event of Default on the part of CLIENT, then OUTSOURCER may, at the sole option of CLIENT, continue to perform such services as may be required by the CLIENT, at its rates then in effect, in order to operate the CLIENT's computing system until such time as an orderly transition may be effected, but no later than 90 days after the Termination Date; provided, however, that if the Event of Default consists in CLIENT's failure to pay any sums due OUTSOURCER, then OUTSOURCER shall continue to perform such services as may be required by the CLIENT after the Termination Date, at OUTSOURCER's

rates then in effect, only if the CLIENT pays for such services in advance.

3.15 Funding:

3.15.1 CLIENT hereby represents to OUTSOURCER that (i) the services to be performed by OUTSOURCER hereunder are necessary to CLIENT's efficient operation of its business and (ii) to the best of its knowledge, after investigation, it believes that sufficient funds may be obtained by it or appropriated for it in order to make all payments contemplated hereby.

3.15.2 CLIENT shall make its best efforts to obtain, or cause to be appropriated as part of CLIENT's annual budget, sufficient funds to pay the sums due from time to time hereunder.

3.16 Independent Contractor Status:

OUTSOURCER and CLIENT acknowledge and agree that OUTSOURCER is and shall be an independent
contractor; that neither OUTSOURCER nor any of its employees, representatives or agents is, or shall be deemed to be, an employee, partner or joint venture of the CLIENT; and that neither OUTSOURCER nor any of its employees, representatives or agents shall be entitled to any employee benefits under any employee benefit plan, including medical, insurance and other similar plans, of the CLIENT. OUTSOURCER further acknowledges that the CLIENT will not withhold any amounts in respect to local taxes
from amounts payable by the CLIENT hereunder and it shall be the exclusive responsibility of OUTSOURCER to pay all amounts due in respect of applicable federal, state and local taxes on such amounts.

3.17 Client Policy and Procedures:

OUTSOURCER agrees to comply with all applicable CLIENT policies and procedures, including but not limited to those regarding conditions of work, access to and use of CLIENT's offices, facilities, work space, support services, supplies, Data Processing Equipment and software and access.

4. MISCELLANEOUS PROVISIONS

4.1 Severability:

Each provision of this Agreement shall be a separate and distinct covenant and, if declared illegal, unenforceable or in conflict with any governing law, shall not affect the validity of the remaining portion of this Agreement.

4.2.1 Client's Contract Administrator:

The CLIENT shall appoint as **Contract** Administrator
_____, who will be delegated the duty and responsibility

of maintaining liaison with OUTSOURCER and to oversee performance of this Agreement.

4.2.2 OUTSOURCER's Contract Administrator:

The Outsourcer shall appoint as **Contract** Administrator
_____, who will be delegated the duty and responsibility of maintaining liaison with CLIENT and to oversee performance of this Agreement.

4.3 Successors:

This Agreement and all future amendments shall be binding on parties and their heirs, successors and assigns. The CLIENT agrees that OUTSOURCER may pledge or assign the net sums of money due and to become due to it hereunder to any bank, lending agency or institution as collateral security.

4.4 Renewal/Extension:

Upon written agreement of both parties entered into at least ninety (90) days prior to the expiration date, this Agreement may be extended for successive one year periods on the terms and conditions then in effect subject however, to such modifications as may be set forth in the extension agreement.

4.5 Entire Agreement-Amendments:

(a) This Agreement, together with the Exhibits hereto, embodies the entire agreement and understanding between the parties hereto and supersedes all prior understandings and agreements, whether written or oral, between the parties hereto relating to the matter hereof.

(b) This Agreement (including the Exhibits hereto) may not be amended or modified except in writing signed by the parties hereto.

4.6 Assignment

This Agreement may not be assigned by either party without the prior written consent of the other party. For the avoidance of doubt, a change of control of OUTSOURCER shall not constitute an assignment for purposes hereof.

4.7 Attorneys Fees

In the event that suit is brought to enforce the provisions of this Agreement, the prevailing party, as determined by the judge, or arbitrator in the event of arbitration, shall be entitled to an award of reasonable attorneys' fees, paralegals' fees and court costs, whether incurred before trial, at trial, during appeals, or in any mediation or arbitration required by a court.