**ANNEX- A**
**Cases related to IT Security in Sri Lanka**

## I. Soft Systems (Pvt.) Ltd, India Vs Microsystems (Pvt) Ltd, Dehiwala

The information is based on the of information of the article published on Daily News, Monday 16, June 2003, http://www.dailynews.lk/2003/06/16/bus05.html, by *Kumar Wethasinghe* with the heading, Commercial High Court dismisses software piracy case

This is the first ever software piracy case in Sri Lanka. In this case Soft Systems (Pvt) Ltd. of Panapilly Nagoor, Kochchi-Kerela-India, obtained an expatriate enjoining order against a local company, Visualtech Microsystems (Pvt) Ltd, Dehiwala, alleging that their source code version of the computer program "Harvest" designed for agri-business activity, had been pirated by the defendants and an identical computer program "Ves-AGRI" had been unlawfully installed.
The defendant moved court in terms of Section 87(1) of Civil Procedure Code.

Commercial High Court Judge of the Western Province L. K. Wimalachandra dismissed the first ever software piracy case when the plaintiff's witness, more particularly the witness under cross examination failed to appear in court without even instructing their own counsel.



## II. Qsoft on Seven Seas Computers

On or about October 2001, Seven Seas Computers Lanka Ltd. (Plaintiff) filed action against Qsoft Ltd. and some of its employees (Defendants) praying for injunctive relief and damages, on the allegation that the Defendants were infringing the intellectual property rights of the Plaintiff by, inter alia, copying their software products, using their trade secrets and by engaging in unfair trade practices. However the court, subject to Seven Seas Computers submitting a bond for One Million Rupees (Rs. 1,000,000) as security, had granted an interim injunction (and not permanent injunction) until the final determination of the case, restraining, inter alia, the Defendants from using or making use of trade secrets of the Plaintiff. This order was given on August 21, 2002. The Court has given this order on the basis that "the object of the interim injunction is to preserve the status quo and prevent future injury.

The source of information is the article published on daily News on Thursday 13 March 2003, http://www.dailynews.lk/2003/03/13/bus07.html, on Qsoft on Seven Seas Computers press release.

# ANNEX -B

## General Structure and IT Structure of Selected Organizations

Information on general Structure and IT structure of organizations selected for the study are as tabulated in Table B.1 and Table B.2I.

| Company | Organizational Structure: | IT Infrastructure: | IT Assets structure |
|---|---|---|---|
| **G1** | Medium scale, hierarchical | Local Area Network connecting divisions in the same building. Point to point WAN link exists with the Ministry head office only for internet connectivity via local proxy server | IT assets of 100 + computers, 10 servers 5 switches and 60 modems. The last year IT budget is 8,100,000 Sri Lankan rupees. The last year IT budget is 8,100,000 Sri Lankan rupees. |
| **G2** | Large scale hierarchical | Organizations divisions are in 6 separate buildings which have their own Local Area Network setup with ADSL connectivity to each building to connect with outside Service Provider for Internet and Email services. And remote divisions are only facilitated with dialup connections. The divisions are not inter-connected. | IT assets of organization includes of ~300 computers, 5 servers with 1 IBM mainframe, 5 switches and 1 router. |
| **G3** | Large scale hierarchical | Organizations divisions are in 6 separate buildings which have their own Local Area Network setup with ADSL connectivity to each building to connect with outside Service Provider for Internet and Email services. And remote divisions are only facilitated with dialup connections. The divisions are not inter-connected. | IT assets of organization includes of ~300 computers, 5 servers with 1 IBM mainframe, 5 switches and 1 router. |
| **G4** | Medium scale hierarchical | The organization has two IT divisions, Division 1 Responsible for IT applicability of organization business function and Division 2 to facilitate the corporate Information technology requirements like, email and Internet connectivity.<br>Division1 has 8 WAN links with dialup connectivity to remote sites and 3 GSM links for Mobile Units. Division2 has only LAN implementation. The two LAN and WAN implementations are physically and logically isolated for security purposes. | The Division-1 consist IT assets of 35 computers, 2 Servers with, 10 switches and 9 routers and 8 modems including assets at remote sites. The Division-2 is equipped with 40 computers 1 server 3 switches and 5 routers.<br><br>Company IT asset values claimed to be of 2Million of Hardware and 3 million of Software |

| | | | |
|---|---|---|---|
| | | | assets. |
| **G5** | Medium scale hierarchical | A structured IT infrastructure is not implemented. The divisions are given with certain IT assets required for operations. The computer room is networked and used store and process reports and house small data bases.<br>Dialup connections are used for Internet and Email facilities where requires | Organization consists of IT Assets of 50 computers 1 server with 5 Switches/hubs and 4 modems. |
| | | | |
| **SG1** | Large scale hierarchical | The network is mainly consists of dummy terminals (about 350) at remote locations connected to Main Frames in the data center via copper connections. A Fiber Optic backbone is in implementation and the Mainframes also will be replaced by New servers. There are 3 separate LANs in three sites that are connected to Data Center using IP connections via leased WAN links.<br><br>The data center connects to service provider using leased internet connection to connect the corporate network to the outside worlds | Organization consists of the IT assets of 450 computers, 4 Servers including 2 Mainframes 25 switches/ routers and 14 modems. |
| **SG2** | Medium scale hierarchical | The IT Data Center located at the Head office premises connects to 15 branch offices over leased WAN links for business related transactions and email and Internet services.<br>Other branches (80) have their own isolated LAN structure and they access internet separately via modem connections.<br>Head office connects to outside with a leased link provided by Service Provider. | Organizations It infrastructure consists of the IT assets of 1500 computers, 250 Servers including 150 switches/ 200 routers and about 150 modems |
| **SG3** | Medium scale hierarchical | The company consists with 21 branch offices. Main business systems and Email servers are maintained at head office data center. All branches are connected to the main office over WAN links for some business system access and Email access. The internet given to some branches by head office and some branches via service providers with direct ADSL connections. | Not provided |
| **SG4** | Medium scale hierarchical | Head office maintains the IT datacenter which consists of main business servers, main and proxy servers. 350 branches are connected to the main office over WAN links for some business | Organizations It infrastructure consists of the IT assets of about 1000 computers, 500 odd Servers including 350 switches/ 400 routers and about 300 |

| | | | |
|---|---|---|---|
| | | system access and Email access. Some branches also access internet via head office proxy server.<br>Branches maintain their own LAN structure and modems to connect to internet. Also there are Severs for application and systems at each branch. | modems. |
| **SG5** | Large scale hierarchical | The head office connects to 50 remote sites over WAN links. All sites maintain their own LAN infrastructure. The corporate users connect to head office for Business application system access, for Email and Internet access. There are some modems connections also at remote offices to connect to Internet when the facility is not granted from head office.<br>The company business is also related to I and Communication and the business is handled by a separate business unit while corporate requirements are managed by separate IT division.<br><br>The organization connects to outside global network via high bandwidth Satellite and Submarine links with a limited bandwidth is dedicated to use of corporate users and other for business customers. | Corporate IT assets consist of 500+ computers, about 50 Servers with servers for company ERP and Billing systems, mail and Internet connectivity 80+ Switches , about 100 Routers and 50+ modems. |
| | | | |
| **P1** | Large scale hierarchical | Six local sites exist with their own LAN implementations with two main Local sites and which hosts and managed all systems and services provided by IT. There are 23 overseas sites with their own LAN structure.<br><br>Local sites are connected with WAN links (leased links and ATM) provided by two ISPs.<br>Overseas sites are connected with head office sites over VPN links provided by international service provider.<br><br>The corporate network is connected from Colombo site to an ISP over a leased link for Internet and outside email connectivity. | IT assets of 3000+ computers, 150 Servers in Local and Overseas sites 50 Switches, 40 Routers and about 25 modems are managed by internal IT division with proper service agreements with hardware vendors. |
| **P2** | Medium scale hierarchical | The IT infrastructure consists of Head office at Colombo and 10 branch offices which owns their own LAN structure. Head office is connected to 10 odd branch offices over WAN links (leased lines | IT assets of 350 computers, 20 Servers in including branch offices 40 Switches ,15 Routers and about 20 modems are managed by internal IT |

| | | | |
|---|---|---|---|
| | | provided by Service Provider) for Emails and necessary business transactions.<br>The head office is connected to global network over a leased connection and grant internet access for corporate users. Branch offices use modem connections to connect to internet where not provided by head office. | department. |
| **P3** | Large scale Matrix structure | The organization consists of 38 sub companies and the master company. All the companies have their own LAN structure and they are all connected in a corporate VPN with frame relay links. The Master company hosts important business systems in two separate data centers in two buildings connected over a WAN link.<br>The sub companies have their own email and Internet connectivity and also they are linked each other. | The company hardware assets consists of IT assets of 1500 computers, 20 Servers in including servers at sub companies and about 50 Switches ,70 Routers and about 30 modems . |
| **P4** | Small scale hierarchical | The physical location of the company limited to two buildings<br>The IT infrastructure consists separate LAN connections in each building and WAN connectivity over fiber link. Infrastructure is managed by one admin unit in head office. | Not Provided |
| **P5** | Small scale hierarchical | The IT infrastructure consists of LAN structure connecting company network in one building. The corporate network is connected to the internet using a leased line connectivity provided by an ISP. | The company hardware assets consist of IT assets of 80 computers, 5 Servers, 5 Switches, 2 Routers and 1 Modem connection. |
| | | | |
| **T1** | Medium scale hierarchical | The IT infrastructure supports the business that related to IT and the corporate users for their day to day operations.<br>7 remote sites with their LAN structure implemented, are connected via company own WAN links. Also remote corporate users connect via dialup connections to the company network.<br>The organization connects to outside global network via high bandwidth Satellite and Submarine links which uses by their business users also. A limited bandwidth is dedicated to use of corporate users | Not Provided |

| | | | |
|---|---|---|---|
| **T2** | Medium scale hierarchical | The Company wide corporate LAN is implemented in one building and connected to few local branch offices over WAN links. Five overseas sites are connected to the head office via VPN connections using dialup.<br><br>Leased links exists to an ISP for Internet and also an ADSL connection from the head office. | IT assets of 200+ computers, 40 Servers 5 Switches ,3 Routers and 5 modems are managed by IT division. |
| **T3** | Medium scale hierarchical | Two offices (Head office and Branch office) are connected over WAN link, a leased line provided by a Service Provider. The WAN links consist of two firewalls in both ends. Both branch offices connect to the internet via a ADSL connection and Head office contains 3 leased lines from a service provider to connect to internet.<br><br>The Email, Internet and IP phone services are provided by company IT division also with business applications | IT assets of 250 computers, 30 Servers 25 Switches ,6 Routers are managed by IT division. |
| **T4** | Medium scale hierarchical | The company VPN provided by Service Provider is connecting two Local and five overseas sites. Each site got their own ADSL connections to connect to the global Network.<br>The IT services to the Local sites are provided by the IT division in the head office in Sri Lanka. | IT assets consists of 1000+ computers, 42 Servers 25 Switches ,5 Routers and 15 modems . Assets are managed by IT division with Service Level agreements with Vendors for maintenance of Hardware Products. |



**Table B.1:** Structure of Organizations

## IT Structure of selected Organizations

| Company | IT Structure | IT Policy |
|---|---|---|
| **G1** | A separate division exists for IT with 75 employees attached. IT Infrastructure and IT systems, Services are partially outsourced, while IT security is managed by the internal IT division | A written Standard exists covering some IT areas for the organization. |
| **G2** | Two divisions for Information Technology with 150 employees attached, Data Processing Division for data processing function (related to organizations main responsibility) and Information Division for information technology (IT) related functions for corporate users. IT Infrastructure and IT systems and IT security Services are partially outsourced. | No written standard or policy exists for IT or IT security in the organization |
| **G3** | Two divisions for Information Technology with 150 employees attached, Data Processing Division for data processing function (related to organizations main responsibility) and Information Division for information technology (IT) related functions for corporate users. IT Infrastructure and IT systems and IT security Services are partially outsourced. | No written standard or policy exists for IT or IT security in the organization |
| **G4** | A separate department exists for IT with 8 employees attached. IT Infrastructure and IT systems and IT security Services are partially outsourced. | No written standard or policy exists for IT or IT security in the organization |
| **G5** | No separate division exists for IT related services and IT Support for a certain level given by assigned officials at HR and training division with one admin personal. IT Infrastructure is fully outsourced while and IT systems and IT security Services are managed by responsible officials to some extend. | No written standard or policy exists for IT or IT security in the organization |
| | | |
| **SG1** | A separate division for exists for IT with 84 employees attached. IT Infrastructure, IT Systems and Services and IT Security are managed by internal IT division. | No written standard or policy exists for IT or IT security in the organization |
| **SG2** | A separate division exists for IT with 60 employees attached. IT Infrastructure and IT systems, Services are partially outsourced, while IT security is managed by the internal IT division. | A written Standard exists for the organization, covering systems security related to Applications, Networks, Database and Physical and Logical Access security. |
| **SG3** | A separate Information Technology division with 20 employees attached IT Infrastructure, IT Systems and Services and IT Security are managed by internal IT division. | A written policy exists for IT covering the areas of, Hardware and software Procumbent, System administration and execution and IT Security |

| | | |
|---|---|---|
| | | system. |
| **SG4** | A separate department exists for IT with 200 employees attached. IT Infrastructure and IT systems and IT security Services are partially outsourced. | A written policy exists for IT covering the areas of E-mail, and other company specific systems. |
| **SG5** | A separate Information Technology department exists with 55 employees attached.<br>IT Infrastructure and IT Security are managed by internal IT division while IT Systems and Services are partially outsourced. | A written policy exists for IT in the organization |
| | | |
| **P1** | A separate division exists for IT with 200 employees attached. IT Infrastructure, IT Systems and Services and IT Security are managed internally by the IT department. | A written standard or policy exists for IT in the organization covering Hardware and Software administration, backup maintenance, Email and internet usage, IT service allocation responsibility and It clearance. |
| **P2** | A separate division exists for IT with 15 employees' attached.. IT Infrastructure and IT systems and Services are partially outsourced, while IT security is managed by the internal IT division. | A written policy exists for the organization covering all IT related areas applicable to the company. |
| **P3** | A separate Information Technology department exists with 23 employees attached.<br>IT Infrastructure and IT Security are managed by internal IT division while IT Systems and Services are partially outsourced. | No written policy exists at present for IT in the organization and it is in the process of implementation. |
| **P4** | A separate department exists for IT with 6 employees attached. IT Infrastructure and IT Security are managed by internal IT division while IT Systems and Services are partially outsourced. | A written policy exists for IT in the organization covering backup procedure and user responsibilities related to the IT resources and services provided |
| **P5** | A separate department exists for IT with 6 employees attached.<br>IT Infrastructure and IT security Services are managed by internal IT division while IT systems and services are partially outsourced. | No written policy exists for IT in the organization. |
| | | |

| | | |
|---|---|---|
| **T1** | A separate division for exists for IT with 15 employees attached. IT Infrastructure, IT Systems and Services and IT Security are partially outsourced. | A written standard or policy exists for IT in the organization covering Hardware, access levels, internet and Email services. |
| **T2** | A separate division exists for IT with 12 employees attached, 7 local administrators and 5 overseas administrators. IT Infrastructure and IT systems, Services are partially outsourced, while IT security is managed by the internal IT division. | A written policy exists for the organization including IT Security. Also the company IT standards are maintained in parallel with CMM standards and ISO standards.<br>The standards are revised in every6 months |
| **T3** | A separate department exists for IT with 8 employees attached. IT Infrastructure and IT systems and IT security Services are managed by internal IT division. | No written policy exists for IT in the organization. |
| **T4** | A separate department exists for IT with 6 employees attached.<br>IT Infrastructure and IT systems are partially outsourced in which the Help Desk is fully out sourced. IT security Services are managed by internal IT division. | A written policy exists for IT covering the areas of Internet Access, E-mail, services and use of IT resources. |



**Table B.2: IT Structure of Organizations**

# ANNEX -C

## Information on Internet and Email Usage in Organizations

### Internet and Email Usage

| Organization | Internet (Users/Accounts) | Internet % (of total staff) | Email (Users /Accounts) | Email % (of total staff) |
|---|---|---|---|---|
| G1 | 240 | 23.70% | 879 | 87.0% |
| G2 | 25 | 5.00% | 25 | 5.0% |
| G3 | 50 | 1.60% | 30 | 2.0% |
| G4 | 50 | 29.00% | 50 | 29.0% |
| G5 | 50 | 4.60% | 50 | 4.6% |
| | | | | |
| SG1 | 100 | 0.80% | 100 | 0.8% |
| SG2 | 100 | 1.10% | 500 | 5.8% |
| SG4 | 22 | 6.00% | 30 | 8.0% |
| SG4 | 150 | 1.50% | 350 | 3.5% |
| SG4 | 400 | 5.70% | 600 | 8.5% |
| | | | | |
| P1 | 630 | 18.00% | 1480 | 42.0% |
| P2 | 50 | 16.00% | 100 | 33.0% |
| P3 | 1000 | 50.00% | 1300 | 65.0% |
| P4 | 16 | 23.00% | 16 | 23.0% |
| P5 | 15 | 15.00% | 50 | 50.0% |
| | | | | |
| T1 | 450 | 90.00% | 450 | 90.0% |
| T2 | 270 | 90.00% | 270 | 90.0% |
| T3 | 250 | 100.00% | 250 | 100.0% |
| T4 | 800 | 100.00% | 800 | 100.0% |
| | | | | |

**Table C.1:** Internet and Email Usage



### Method of Connection to Internet (Outside Networks)

| Organization | Method of Connection |
|---|---|
| G1 | Leased line from service provider. |
| G2 | Point to Point Frame relay connection from the Ministry |
| G3 | ADSL connection from ISP to 6 divisional locations.<br>Few Dialup connections to other locations |
| G4 | Leased line from service provider. |
| G5 | ISP leased line connectivity/Few dialup connections |

| | |
|---|---|
| SG1 | Leased line from service provider & Dialup Connections |
| SG2 | Leased line from service provider & Dialup Connections |
| SG4 | Leased line from service provider & Dialup Connections |
| SG4 | Leased line from service provider & Dialup Connections |
| SG4 | Leased Line connection (direct) |
| | |
| P1 | Leased lines from service provider |
| P2 | Leased lines from service provider |
| P3 | Leased lines from service provider |
| P4 | Leased lines from service provider |
| P5 | ADSL connection from ISP |
| | |
| T1 | Leased line from service provider. |
| T2 | ADSL connection to ISP. |
| T3 | Leased Line connection & ADSL connection to ISP |
| T4 | Leased Line connection & ADSL connection to ISP |
| | |

**Table C.2:** Method of connection to Internet/External Email



**Internet Usage Comparison**

| Organizations | Connection | Restrictions | Virus Protection | Internet Policy | Usage |
|---|---|---|---|---|---|
| **G1** | Through Proxy (ISA) & Software Firewall | Allowed for selected user base (240)<br><br>site restrictions<br><br>content restrictions | PC Virus scanners<br><br>Server side protection | A Policy Exists (A Circular) | Information gathering<br><br>Information Publishing |
| **G2** | Through a proxy. (Direct connection from Head office | Allowed for selected user base | PC Virus scanners only | A Policy Exists | Information gathering<br><br>Information Publishing |
| **G3** | Direct from Service Provider (ISP) | Allowed for selected user base (20) | PC Virus scanners only | None | Information gathering Information Publishing |

| | | | | | |
|---|---|---|---|---|---|
| **G4** | Through Proxy (ISA) & Hardware Firewall | Allowed for selected user base | PC Virus scanners only | None | Information gathering<br><br>Information Publishing |
| **G5** | Direct from Service Provider (ISP) | Allowed for selected user base | PC Virus scanners only | None | Information gathering<br><br>Information Publishing |
| | | | | | |
| | | | | | |
| **SG1** | Through Proxy (ISA) & Hardware Firewall | Allowed for selected user base | PC Virus scanners<br><br>Server side Virus protection | None | Customer inquiry and requests management<br><br>Information gathering<br><br>Information Publishing |
| **SG2** | Dialup connection | Allowed for selected user base | PC Virus scanners | Yes | Customer inquiry and requests management<br><br>Information gathering<br><br>Information Publishing |
| **SG3** | Through Proxy & Hardware Firewall | Allowed for selected user base<br><br>Time restrictions | PC Virus scanners<br><br>Server side Virus protection | Yes | E-commerce,<br><br>Customer payments<br><br>Information gathering<br><br>Information Publishing |
| **SG4** | Through Proxy & Software Firewall | Allowed for selected user base | PC Virus scanners<br><br>Server side | Yes | Information gathering<br><br>Information |

| | | | | | |
|---|---|---|---|---|---|
| | | | Virus protection | | Publishing |
| **SG5** | Through Proxy & Software Firewall | Allowed for selected user base<br><br>Site and contents restricted | PC Virus scanners | Yes | Information gathering For R&D work<br><br>Information Publishing |
| | | | | | |
| **P1** | Through Proxy (ISA) & Software Firewall | Allowed for selected user base<br><br>Site & Content Restrictions | PC Virus scanners<br><br>Back-end Virus filtering for HTTP/HTTPS/ FTP | Yes | Information gathering for R&D<br><br>E- commerce for some extent<br>Information Publishing |
| **P2** | Through Proxy & Hardware Firewall | Allowed for selected user base<br><br>Site and contents restricted | PC Virus scanners<br><br>Back-end Virus filtering | Yes | Information gathering<br><br>Customer inquiry management<br><br>Information Publishing |
| **P3** | Through Proxy & Hardware Firewall | Allowed for selected user base | PC Virus scanners<br><br>Server Virus Scanners | No | Information gathering For R&D work<br>Information Publishing |
| **P4** | Through Proxy & Hardware Firewall | Allowed for selected user base | PC Firewalls | Yes | Information gathering For R&D work<br>Information Publishing |
| **P5** | Direct from ISP | Allowed for selected user base | PC Virus scanners<br><br>Router level filtering | Yes | Information gathering For programming<br>Operational data download<br>Information Publishing |

| | | | | | |
|---|---|---|---|---|---|
| **T1** | Through Proxy (ISA) & Hardware Firewall | Allowed for selected user base<br><br>Site & Content Restrictions | PC Virus scanners | Yes | Information gathering |
| **T2** | Through Proxy & Software Firewall | Site and contents restricted<br><br>(All Users are allowed ) | PC Virus scanners<br><br>(on access scanning configured) | Yes | To connect to Overseas branch offices<br><br>Information gathering |
| **T3** | Through Proxy & Software Firewall | No restriction | PC Virus scanners<br><br>Server side Virus protection | Yes | Information gathering For R&D work |
| **T4** | Through Proxy & Software Firewall | Site and contents restricted (All Users are allowed ) | PC Virus scanners (on access) Server side Virus protection | Yes | Information gathering For R&D work |



**Table C.3:** Internet Usage Comparison

## Email Usage Comparison

| Organization | Email Architecture | Restrictions | Virus Protection | Email Policy |
|---|---|---|---|---|
| **G1** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | Allowed for selected user base (879)<br><br>File Type restrictions<br><br>External Attachment size restrictions | PC Virus scanners<br><br>Server Virus Scanners | None |
| **G2** | From Service Provider | Allowed for selected user base<br><br>File Type & Attachment size restrictions (Service provider standards) | PC Virus scanners only | None |

| | | | | |
|---|---|---|---|---|
| **G3** | From Service Provider | Allowed for selected user base (50)<br><br>File Type & Attachment size restrictions (Service provider standards) | PC Virus scanners only | None |
| **G4** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | Allowed for selected user base (50)<br><br>No restrictions in place | PC Virus scanners only | None |
| **G5** | From Service Provider | Allowed for selected user base (30)<br><br>File Type & Attachment size restrictions (Service provider standards) | PC Virus scanners only | None |
| | | | | |
| **SG1** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | Allowed for selected user base<br><br>File Type restrictions (.exe, zip)<br><br>Attachment size restrictions (internal/external) | PC Virus scanners<br><br>Server Virus Scanners | None |
| **SG2** | From Service Provider | Allowed for selected user base<br><br>(Service provider standards) | PC Virus scanners only | None |
| **SG3** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | External email access for all users<br><br>Attachment size restrictions.<br><br>File Type Restrictions (.JPG,.MP3, DAT, .EXE) | PC Virus scanners<br><br>Server Virus Scanners | None |
| **SG4** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | Allowed for selected user base<br><br>Attachment size restrictions. | PC Virus scanners<br><br>SMTP Isolations by gateway | Yes |

| | | | | |
|---|---|---|---|---|
| **SG5** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | External email access for all email users<br><br>Attachment size restrictions.<br><br>File Type Restrictions (.jpg,.mp3,.dat,.exe) | PC Virus scanners<br><br>Email Virus Scanner at server end | None |
| | | | | |
| **P1** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | Allowed for selected user base for external mail<br><br>File Type restrictions<br><br>Attachment size restrictions (internal/external) | PC Virus scanners<br><br>Mail Server Virus Scanners<br><br>Back-end SMTP filtering for virus | Yes |
| **P2** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | Allowed for selected user base for external mail<br>File Type restrictions<br><br>Attachment size restrictions (internal/external) | PC Virus scanners<br><br>Mail Server Virus Scanners | Yes |
| **P3** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | Allowed for selected user base for external mail<br><br>Attachment size restrictions for external (20MB). | PC Virus scanners<br><br>Email Virus Scanner at server end | None |
| **P4** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | None<br><br>(Allowed for all users with external email) | PC Virus scanners<br><br>Mail Server Virus scanners | Yes |
| **P5** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | Attachment size restrictions (internal/external)<br><br>All users are allowed for internal mail<br><br>Selected users for external mail | PC Virus scanners | Yes |
| | | | | |
| **T1** | Corporate Email Architecture Implemented<br><br>(Authenticated | Allowed for selected user base<br><br>File Type restrictions | PC Virus scanners | Yes |

| | | | | |
|---|---|---|---|---|
| | access) | Attachment size restrictions (internal/external) | | |
| **T2** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | Attachment size restrictions (internal/external)<br><br>All users are allowed | PC Virus scanners only<br><br>Mail Server Virus Scanners | Yes |
| **T4** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | External email access allowed for selected user base<br><br>Attachment size restrictions. (8MB) | PC Virus scanners<br><br>Mail Server Virus scanners | None |
| **T5** | Corporate Email Architecture Implemented<br><br>(Authenticated access) | Attachment size restrictions. (6MB)<br><br>File Type Restrictions (.exe)<br><br>All users are allowed | PC Virus scanners<br><br>Mail Server Virus scanners | Yes |

**Table C.4:** Email Usage Comparison

# Annex-D

## IT Resource Structure of Organizations

### I. IT Resource Levels

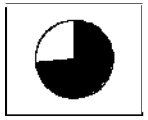
Legend: ● **Adequate** × **Not adequate** **M - manageable**

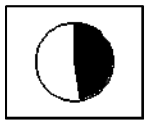
| | G1 | G2 | G3 | G4 | G5 | SG1 | SG2 | SG2 | SG3 | SG4 | P1 | P2 | P2 | P3 | P4 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **IT staff** | × | ● | ● | ● | No IT Staff | ● | ● | ● | ● | ● | **M** | × | ● | × | × | **M** | × | ● | × |
| **Skill Level of IT** | ● | ● | ● | ● | × | ● | × | ● | ● | × | ● | ● | ● | × | ● | ● | ● | ● | × |
| **IT Resources** | × | × | ● | × | × | ● | × | ● | ● | ● | ● | × | ● | × | × | ● | × | ● | × |

**Table D.1:** IT Resource Levels



| | Adequate | Not adequate | Manageable |
|---|---|---|---|
| IT Staff | 10 | 7 | 2 |
| Skill Level of IT | 14 | 5 | - |
| Resources | 9 | 10 | - |





| | |
|---|---|
| | Adequate |
| | Not adequate |
| | Manageable |

**Table D.2:** IT Resource Levels Summary

## II. Outsourcing Information

Legend: IT – Managed by internal IT
P – Partially Outsourced
F – Fully Out sourced

| organization | IT Infrastructure | IT Systems & Services | IT Security Management |
|---|---|---|---|
| G1 | IT | P | IT |
| G2 | P | P | IT |
| G3 | P | P | P |
| G4 | P | P | P |
| G5 | F | P | IT |
| | | | |
| SG1 | IT | IT | IT |
| SG2 | P | P | IT |
| SG3 | IT | IT | IT |
| SG4 | P | P | P |
| SG5 | IT | P | IT |
| | | | |
| P1 | IT | P | P |
| P2 | P | P | IT |
| P3 | IT | P | IT |
| P4 | IT | P | IT |
| P5 | IT | P | IT |
| | | | |
| T1 | P | P | P |
| T2 | P | P | IT |
| T3 | IT | IT | IT |
| T4 | P | P | IT |

**Table D.3:** Outsourcing Information



| | Managed by IT | Partially Outsourced | Fully Out sourced |
|---|---|---|---|
| **IT Infrastructure** | 9 | 9 | 1 |
| **IT Systems & Services** | 3 | 16 | - |
| **IT Security** | 14 | 5 | - |

**Table D.4:** Outsourcing Information Summary

## III. Interest and Commitment from Upper Management

| Organization | Interest towards IT Ethics and Information Sensitivity in organization | Level of commitment and support from higher management related to IT |
|---|---|---|
| **G1** | Satisfactory | Fair |
| **G2** | Satisfactory | Satisfactory |
| **G3** | Fair | Fair |
| **G4** | Fair | Not at all |
| **G5** | Fair | Not at all |
| **SG1** | Fair | Fair |
| **SG2** | Satisfactory | Not at all |
| **SG3** | Satisfactory | Fair |
| **SG4** | Satisfactory | Satisfactory |
| **SG5** | Fair | Not at All |
| **P1** | Satisfactory | Satisfactory |
| **P2** | Fair | Satisfactory |
| **P3** | Fair | Fair |
| **P4** | Fair | Satisfactory |
| **P5** | Fair | Satisfactory |
| **T1** | Satisfactory | Satisfactory |
| **T2** | Satisfactory | Satisfactory |
| **T3** | Satisfactory | Fair |
| **T4** | Satisfactory | Satisfactory |

**Table D.5 :** Interest and Commitment from Upper Management

## IV. User Awareness

| Organization | Conduct of User awareness Programs on IT | Assessment on IT and IT Security | Conduct of outside consultancy or audit |
|---|---|---|---|
| G1 | Yes One time | Yes | Yes |
| G2 | Yes | Yes | No |
| G3 | Yes | No | No |
| G4 | Yes | No | No |
| G5 | No | No | No |
| | | | |
| SG1 | Yes on going | Yes | No |
| SG2 | Yes on going | Yes | No |
| SG3 | Yes one time | Yes | No |
| SG4 | Yes on going | Yes | No |
| SG5 | Yes on going | No | No |
| | | | |
| P1 | Yes on going | yes | yes |
| P2 | Yes on going | yes | yes |
| P3 | Yes on going | yes | yes |
| P4 | Yes one time | yes | no |
| P5 | Yes on going | yes | no |
| | | | |
| T1 | Yes one time | no | yes |
| T2 | Yes one time | no | no |
| T3 | Yes one time | no | no |
| T4 | Yes one time | yes | no |



**Table D.6 :** User Awareness

| | Yes | No |
|---|---|---|
| **Conduct of User awareness Programs on IT** | **18** | **1** |
| **Assessment on IT and ITT Security** | **12** | **7** |
| **Conduct of outside consultancy or audit** | **5** | **14** |

**Table D.7:** User Awareness-Summary

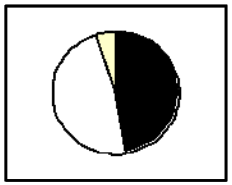
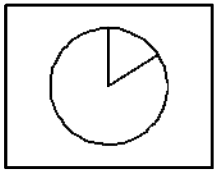
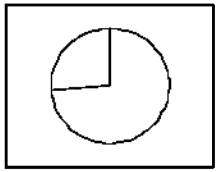
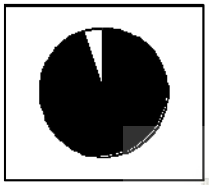
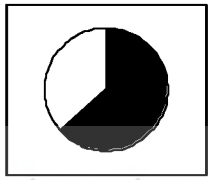
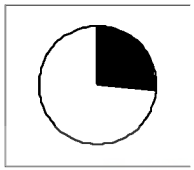
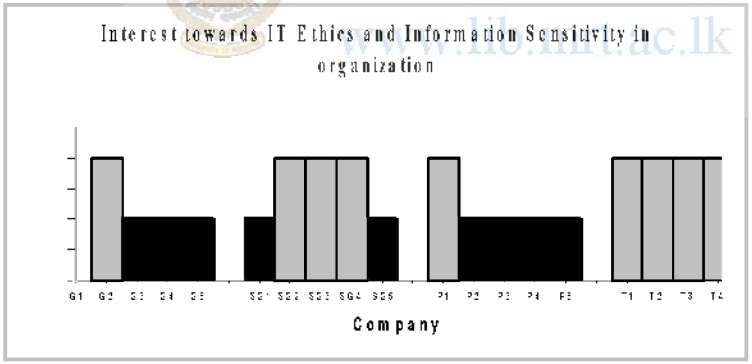
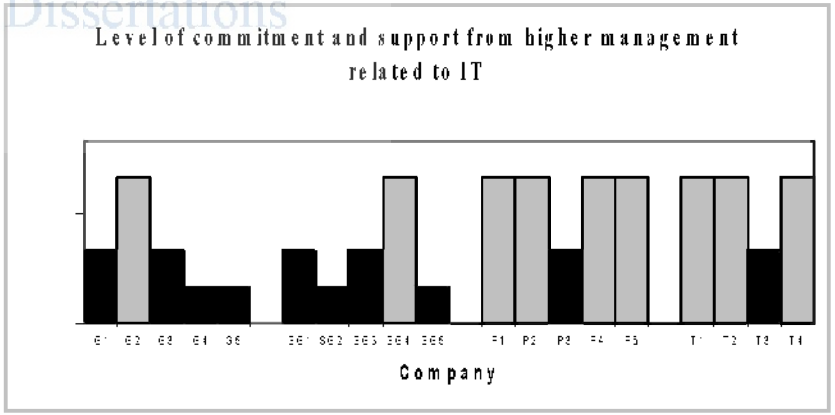
| | | | | |
|---|---|---|---|---|
| **Outsourcing Information** |  **IT Infrastructure** |  **IT Systems & Services** |  **IT Security** | Managed by internal IT<br>Partially Outsourced<br>Fully Outsourced |
| **Interest and Commitment from Upper Management** |  **Conduct of User Awareness Programs** |  **Assessment** |  **Conduct of outside Consultancy or Audit** | Yes<br>No |
| **User Awareness** |   | |   | |
| | Satisfactory | Fair | Not at All | |

**Table D.8:** Out sourcing /Interest and Commitment from Management/User Awareness-Comparison

# ANNEX E - Computer Systems Security in Organizations

## I. System Access Control

a.) Password Protection and Authentication

**A** – Always **S** – Some times **N** - None

| | | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Servers & Admin Computers** | Passwords Login for Systems | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| | Password Login for Application | A | S | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| | Folder Permission | A | S | S | A | A | A | A | A | S | A | A | A | S | A | A | A | A | A | A |

**Table E.1:** Password Protection and Authentication -Servers and Admin Computers

| **server and Admin Computers** | A | S | N |
|---|---|---|---|
| Passwords Login for Systems | 19 | | |
| Password Login for Application | 18 | 1 | |
| Folder Permission | 15 | 4 | |

| **User Computers** | A | S | N |
|---|---|---|---|
| Passwords Login for Systems | 11 | 8 | |
| Password Login for Application | 10 | 8 | 1 |
| Folder Permission | 6 | 10 | 3 |

| | | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **User Computers** | Passwords Login for Systems | S | A | S | A | S | A | A | A | S | S | A | A | S | A | A | A | S | S | A |
| | Password Login for Application | A | S | S | A | A | N | A | A | S | S | A | A | A | S | A | A | S | S | S |
| | Folder Permission | S | S | N | S | N | S | A | A | S | S | A | S | S | A | A | A | S | N | S |

**Table E.2:** Password Protection and Authentication - User Computers

**Y – Yes** **N- No/ No Standard** **W- Written and in -place** **V- Verbal**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Database Protection by Passwords | Y | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | N | Y | Y | Y | Y | N |
| | | | | | | | | | | | | | | | | | | | |
| Third Party Access to Systems | W | V | V | V | N | V | V | W | W | W | W | W | V | V | V | W | V | W | V |

**Table E.3:** Database Protection and Third Party Access

| | y | N |
|---|---|---|
| **Database Protection by Passwords** | 15 | 4 |

| | W | V | N |
|---|---|---|---|
| **Third party Access to software systems** | 8 | 10 | 1 |



b. ) Network Drives &Remote access to systems

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Network Drive Access** | y | y | y | y | N | y | y | y | y | y | y | y | y | y | y | y | y | y | y |
| **Remote Access to Servers to Servers computers and Network equipment** | y | N | N | N | N | y | y | y | y | y | y | y | y | y | y | N | y | y | y |

**Table E.4:** Network Drives &Remote access to systems

| | y | N |
|---|---|---|
| **Network Drive Access** | 18 | 1 |
| **Remote Access to Servers to Servers computers and Network equipment** | 14 | 5 |

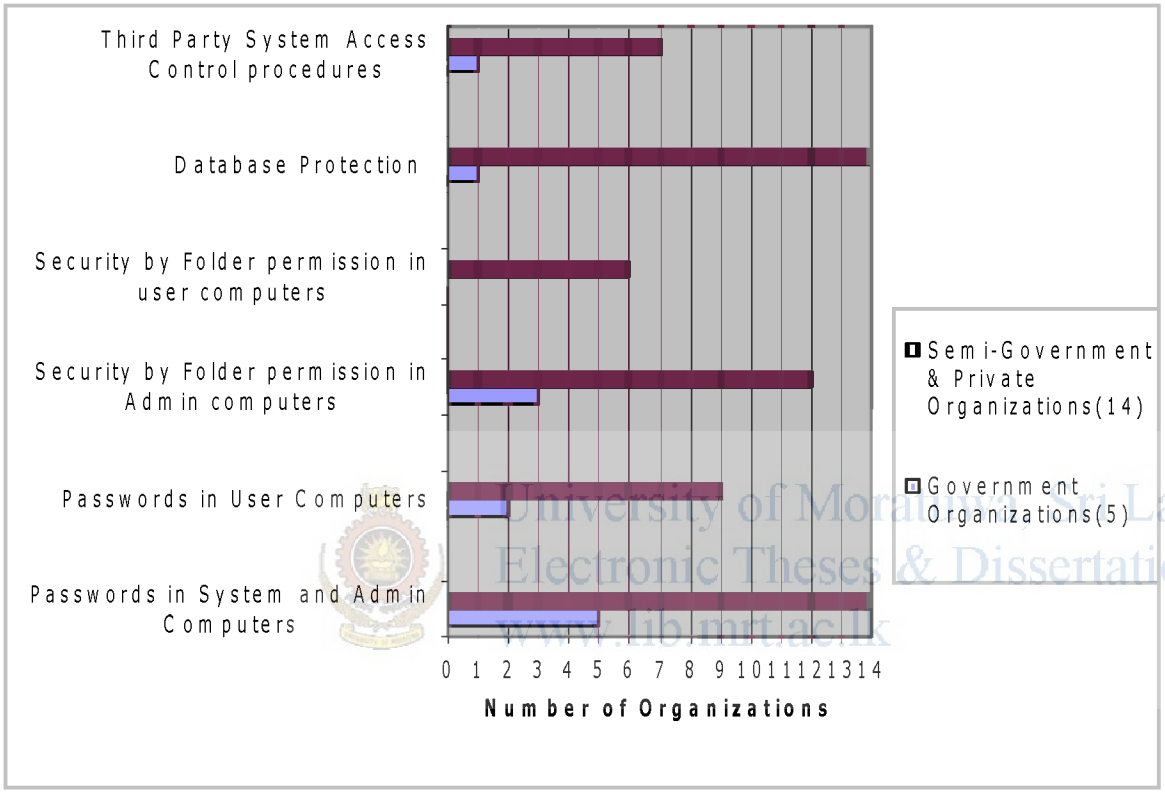
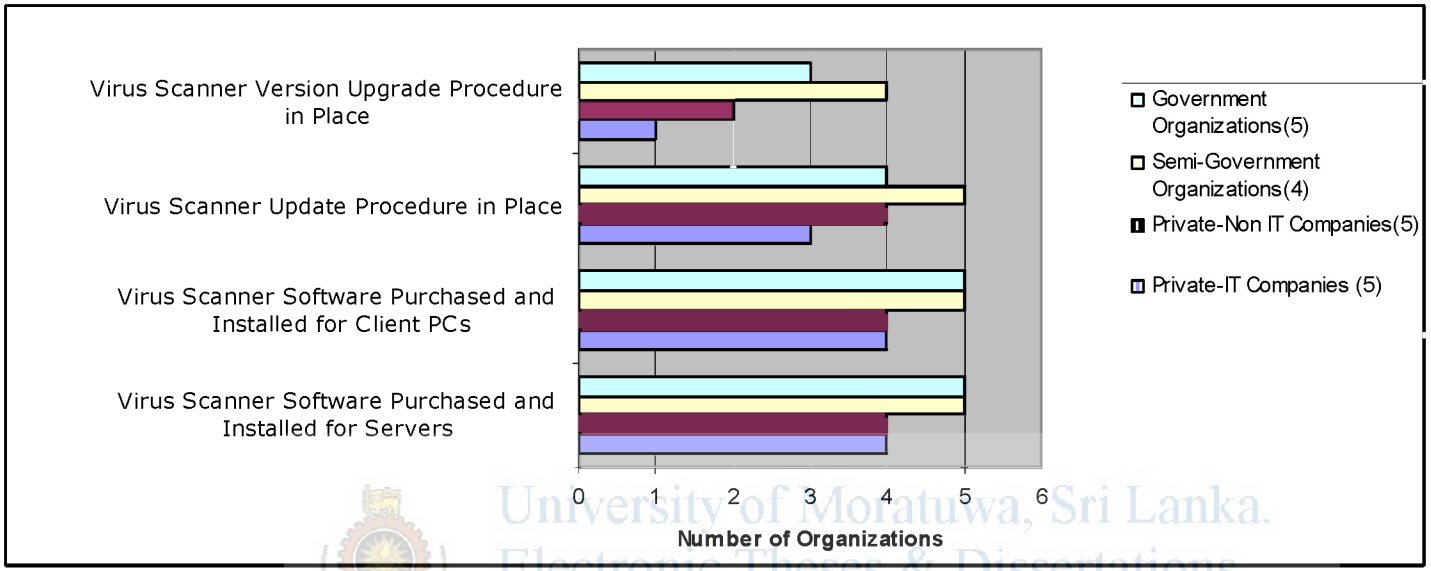





**Figure E.1:** System Access Control –Summary and Comparison



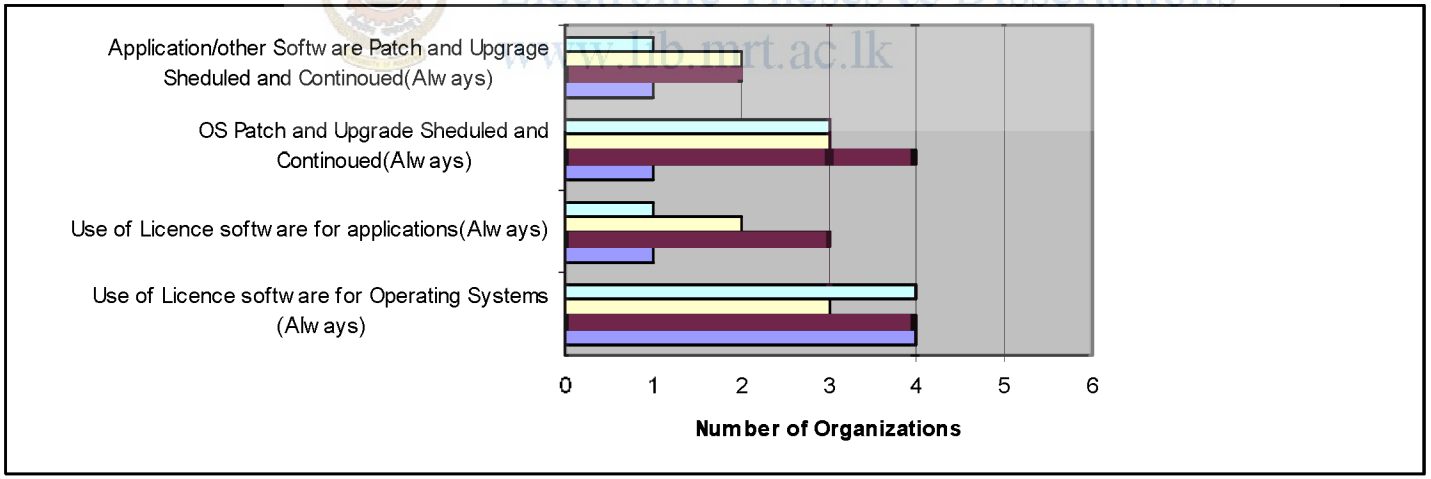






**Figure E.2:** Virus Scanner Installations and System Maintenance -Comparison

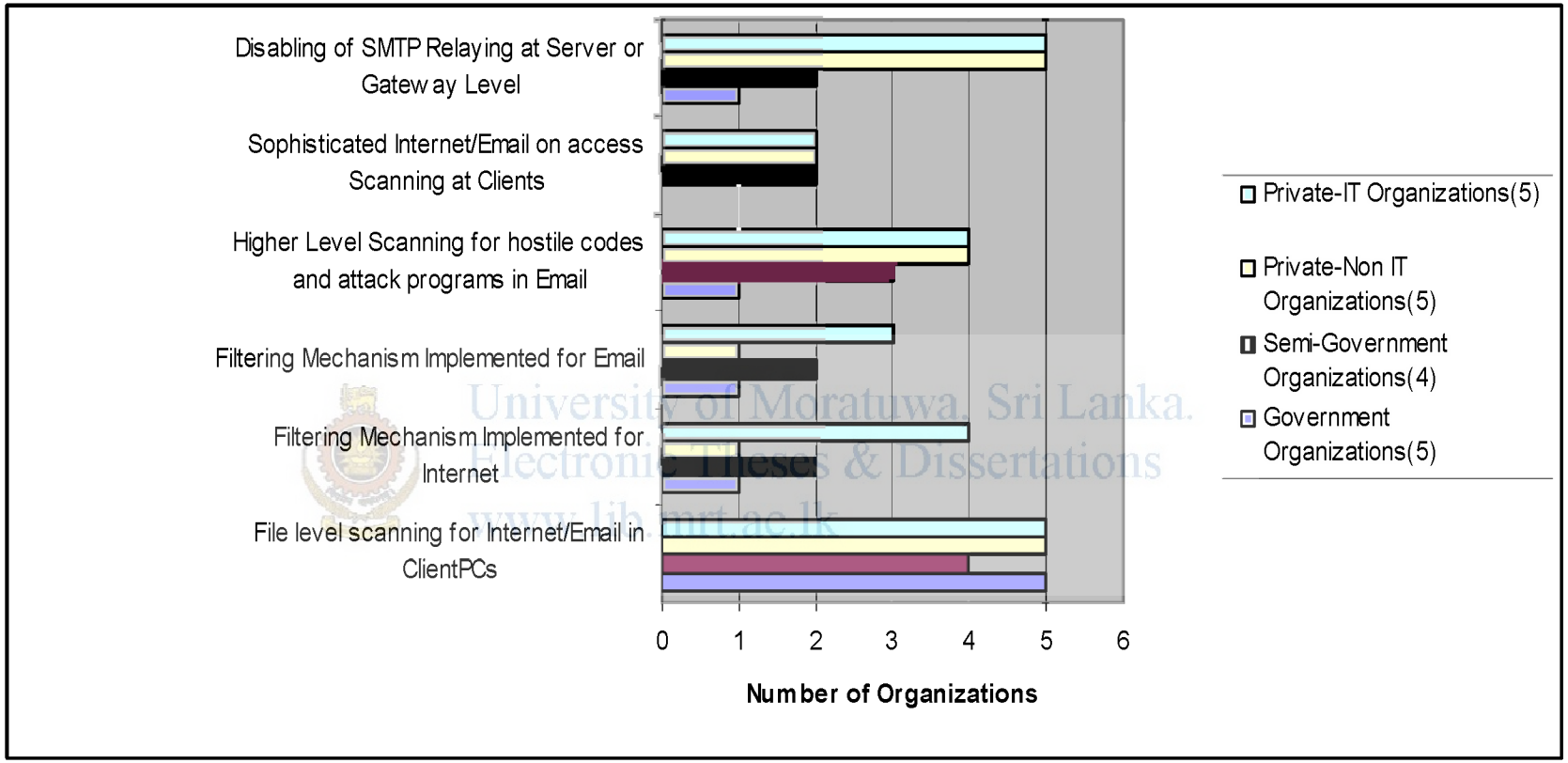





**Figure E.3:** Security in Internet and Email Usage - Comparison

## V. Web Server Related Security

a.) Web server setup and Maintenance

**I** - Internal
**O** - Out sourced
**N** – No Standard Procedure
**P** - Procedure in place

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Web server Implementation** | O | I | O | O | O | I | I | I | I | I | I | O | I | I | I | I | I | I | I |
| **Content Update** | O | I | I | O | O | I | I | I | I | I | I | O | I | I | I | I | I | I | I |
| **Patch update** | - | N | - | - | - | P | N | N | P | N | P | - | P | P | N | N | N | N | N |



**Table E.5:** Web Server Related Security

| | G | SG | P | T | Y | N | N/A |
|---|---|---|---|---|---|---|---|
| web servers | 1 | 5 | 4 | 4 | 14 | | 5 |
| web server Content Updates | 2 | 5 | 4 | 4 | 16 | | 4 |
| Web Server patch updates | 0 | 2 | 3 | 0 | 5 | | 5 |
| secure | | 1 | 1 | 2 | | | |

b.) Intranet and Extranet Implementations

**Y – Yes (Access control in place)** **C – Restricted Corporate access**

**N – No** **S - Secure Internet Access**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Intranet Implementation** | Y o | Y I | N | N | N | Y I | Y I | Y I | N | Y I | Y I | Y I | Y I | Y I | N | Y I | Y I | Y I | Y I |
| **Intranet site access** | C | C S | - | - | - | C S | C | C | C | C | C S | C | C | C S | - | C | C S | C S | C S |
| **Extranet Implementation** | Y | N | N | N | N | N | N | N | N | N | N | Y | N | N | N | N | N | Y | N |
| **Extranet site access** | Y | - | - | - | - | - | - | - | - | - | - | Y | - | - | - | - | - | Y | - |



**Table E.6:** Intranet and Extranet Implementation Security

# Annex -F Physical and Environmental Security

## a.) Hardware Placement

**DC – data center** **SS- Separate Section** **PA- Public Area**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Servers** | DC SS | DC | DC | SS | SS | SS | DC | SS | DC | SS | DC | DC | DC | DC | SS | DC | DC | DC | DC |
| **Computers** | PA | DC | PA SS | PA SS | PA SS | PA | PA | PA SS | PA SS | PA SS | PA | PA | PA SS | PA SS | SS | PA SS | PA SS | PA | PA SS |
| **Network Equipment** | SS | DC SS | SS | SS | SS | SS | SS | SS | SS | SS | DC SS | DC | DC | SS | SS | DC | DC | DC | DC |
| **IT Accessories** | PA | DC | PA SS | SS | SS | PA | PA | PA | SS | PA SS | PA | PA | PA SS | PA SS | PA SS | PA SS | SS | PA | DC SS |

**Table F.1:** Hardware Placement



## b.) Physical Access Control

**W**- Written and In- place **V** – Verbal Standards **N** – Standards **Y c**- Yes /Card reader **Y b** – Yes/ Biometric

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P 5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Access Control to IT Special IT Premises** (Data center, Server Room, Network room) | W | W (S) | V | V | V | W | W | W | W | W (S) | W | W | V | W | W | W | W | W | W |
| **Third-party Access to IT Premises** | W | W | V | V | V | V | W | W | W | | W | W | V | W | V | W | V | V | W |
| **Special Authentication mechanisms** | Y c | - | - | - | - | - | Y b | - | - | - | Y c | - | - | - | - | Y c | Y b | Y c Y b | Y c Y b |

**Table F.2:** Physical Access Control

# Annex -G
# Procedural Security

## I.) Power AC and Temperature Control

a.) Use of reliable power **U – UPS Power** **D- Direct Power**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Servers** | U | U | U | U | U | U | U | U<br>D | U | U | U | U | U | U | U | U | U | U | U |
| **computers** | U<br>D | D | U | U | D | U<br>D | U | D | U | U | U | U | U | U | U | U | U | U | U |
| **Network Equipment** | U | D | U<br>D | U | D | U | U | U<br>D | U | U | U | U | U | U | U | U | U | U | U |
| **Other Equipment** | U<br>D | D | D | U | D | D | U | U<br>D | U | U | U | U<br>D | U | U | U | U | U | U | U |



**Table G.1:** Use of Reliable power for systems

b.) Monitoring of Power, AC, Temperature

**W-** Written in-place **V-** Verbal Standards **N-** No Standard **IP**-in Progress

| | | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Monitoring** | **Power** | V | V | V | V | N | V | V | W | V | V | W | V | V | W | N | W | V | V | W |
| | **AC** | W | V | V | V | N | V | V | V | W | V | W | V | V | V | N | W | IP | W | W |
| | **Temperature** | W | V | V | V | N | V | V | W | N | V | W | V | V | V | N | W | IP | W | W |
| | | | | | | | | | | | | | | | | | | | | |
| **Escalation** | **Power** | V | V | N | V | N | V | V | V | V | V | W | V | V | V | N | W | N | W | V |
| | **Ac** | V | V | N | V | N | V | V | W | V | V | W | V | V | V | N | W | N | N | V |
| | **Temperature** | W | V | N | V | N | W | V | W | V | V | W | V | V | V | N | W | N | N | V |

**Table G.2:** Monitoring of Power Air-conditioning and Temperature



c.) Access Control Mechanisms for Power/Ac

**W-** Written in-place **V-** Verbal Standards **N-** No Standard

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Power Equipment** | W | V | V | V | V | V | W | W | N | N | W | N | V | W | W | W | W | V | V |
| **AC Equipment** | W | V | V | V | V | V | W | V | N | N | W | N | V | V | W | W | N | V | V |

**Table G.3:** Access Control Mechanism for Power /Air Conditioning

## II.) Backup & Disaster Recovery

a.) Backup Maintenance **Y –Yes** **N- No/No Formal Procedure** **RP-** Regular and Procedure in Place

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Hardware Backups** | Y | Y | Y | Y | N | Y | N | Y | N | Y (S) | Y | N | Y | Y (S) | Y | Y | Y (S) | Y | Y |
| **Software Backups** | Y | N | N | N | N | Y | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y |
| **Data backups** | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| | | | | | | | | | | | | | | | | | | | |
| **Backup Status** | RP | RP | RP | RP | NP | RP | RP | RP | RP | | RP | RP | RP | NP | RP | RP | RP | RP | RP |
| **Use of special software** | Y | N | Y | Y | N | N | N | Y | Y | | Y | N | Y | Y | N | Y | Y | Y | Y |
| **Status Monitoring** | RP | RP | RP | N | N | RP | RP | RP | RP | | RP | RP | RP | RP | RP | RP | RP | RP | RP |
| **Backup Retention** | RP | RP | N | N | N | RP | RP | N | N | | RP | RP | RP | RP | RP | RP | RP | RP | RP |
| **Media Used** | T CD | T | T CD | T CD | d | T | T HD | T | T CD | | T CD HD | T HD | T HD USB | T CD HD | T CD | T | T | T | T Tlib |

**Table G.4:** Backup Maintenance

b.) Disaster Recovery **Y –Yes** **N- No**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Protection and DR methods** | **B/U Fai Tests, Proce** | **BU** | **BU** | **BU HWRe .** | - | **B/U** DR plan | **B/U** | **B/U** | **BU HW Re.** | **BU HW Re.** | **B/U** DR plan | **B/U** DR plan | **B/U** DR plan | **B/U** DR plan | **B/U HW Re** DR plan | **BU** DR plan | **BU HW Re.** | **BU** DR plan | **BU** DR plan |
| **DR sites** | **Y** | **-** | - | **Y (HD)** | - | **Y** | **Y** | **Y** | **-** | | - | - | - | - | - | - | - | - | - |

**Table G.5:** Disaster Recovery



**III.) IT Security Procedures**

a. ) Procedure for Physical Access Control and Environment

**P –** Procedure in Place **N -** No Formal Procedure **W –** Written Standard **V-** Verbal standards

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Access Control violation Escalation** | **P** | **V** | **V** | **N** | **N** | **N** | **N** | **P** | **P** | **V** | **P** | **P** | **V** | **V** | **V** | **P** | **V** | **P** | **P** |
| **Track or removal of IT Assets** | **P** | **N** | **P** | **N** | **P** | **N** | **P** | **P** | **P** | **N** | **P** | **P** | **N Strict** | **N** | **P** | **P** | **P** | **N** | **P** |
| | | | | | | | | | | | | | | | | | | | |
| **Guidelines for AC/Power failure in IT areas** | **W-t** | **V** | **N** | **V** | **N** | **V** | **V** | **W-t,p** | **V** | **W P** | **W** | **V** | **V** | **V** | **W P** | **W** | **N** | **V** | **V** |

**Table G.6:** Procedure for Physical Access Control and Environment

b.) Hardware and Software Maintenance

**H- Hardware** **S- Software/Services** **N – None/ No formal Procedure** **Y- Yes /Procedure in Place**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Status Monitoring** | H S | H S | H S | N | N | N | H S | H S | H S | H S | H S | H S | H S | H S | S | H | N | H | N |
| **status Escalation** | Y | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y |
| | | | | | | | | | | | | | | | | | | | |
| **Use of special tools for Monitoring** | Y | N | N | N | N | N | N | Y | N | N | Y | N | N | Y (S) | Y (H) | Y | N | Y | Y |
| **Tools for security loop hole reveal** | Y | N | N | N | N | N | N | N | N | Y | Y | Y | N | Y | Y | N | N | N | Y |
| | | | | | | | | | | | | | | | | | | | |
| **SLA Maintenance** | Y | Y ( H) | Y ( H) | Y | Y | Y (S) | Y | Y | Y | Y | Y (H) | Y | Y | Y | Y (H) | Y | Y | Y | Y |

**Table G.7:** Hardware and Software Maintenance

**III.) IT Security related Incidents**

a.) Down Times and Data Losses **Y -Yes** **N - No** **A- within acceptable limits**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Loss of data or Information ( in last 3 years)** | N | N | N | N | N | Y once | N | N | N | N | Y A | N | Y PC Level | N | Y once | Y 1,2 | Y 1(2) | Y (4) | N |
| **Unscheduled down times reported** | Y A | Y A | Y (2days) | Y A | Y | Y once | Y once | Y once | Y | N | Y A | Y A | Y A | Y A * | Y | Y A | N | N | Y |

**Table G.8:** Down Times and Data Losses for past 3 years



b.) IT Security Violations **Y -Yes** **N - No** **A- within acceptable limits**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **IT Security Violations Reported** | N | N | N | N | Y (Virus) | N | N | N | N | Y Internal ** | Y Internal ** | N | N | N | Y Internal ** | N | Y Int. ** | Y Int. ** | Y Ex ** |
| **Impact by such incidents** | - | - | - | - | Less | - | - | - | - | P | Productivity and Financial | | | | P & F | - | P | No Im. | No Im. |
| **Policy or procedure agreed for security violation** | N | N | N | N | N | Y | N | Y | N | N | Y | Y | N | N | Y | N | N | N | N |

**Table G.9:** IT Security Violations

**** - Acted according to company legal framework**

## IV.) IT Security Policy Implementation

a.) Policy Implementation

**Y -Yes /Practiced and Procedure in place** **N – No/No Formal procedure** **IP- In Progress**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Existence of IT Policy** | Y | Y | N | N | N | N | Y | Y | Y | N | Y | Y | N IP | N ** | Y | Y | Y | Y | Y |
| **existence of IT Security Policy or section in IT policy for security** | N | N | N | N | N | N | Y | Y | N | N | Y | Y | N | Y | Y | Y | Y | Y | Y |

**Table G.10:** Policy Implementation in Organizations

** Not properly enforced



b.) Password Policy

**W- Written and in place** **V- Verbal Standards** **N- No Formal Standard**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **System passwords** | W | V | V | V | N | N | W | W | W | V | W | W | V | W | W | W | V | V | W |
| **Application passwords** | V | V | V | V | N | N | W | W | W | V | W | W | V | W | W | W | V | V | W |
| **Network Equipment passwords** | N | N | V | V | N | N | W | W | W | N | W | V | V | W | V | W | V | V | W |

**Table G.11:** Password Policy

# Annex -H Network and Communication Security

## I.) Perimeter Security

a.) Firewall Implementation and Network Isolation

**F/S** – Firewall Software **F/H** – Firewall Hardware **Y-** Yes **A-** Only Necessary ports allowed **S-**Some ports blocked **P** –Procedure in Place
*** - DMZ Zone** **N-** None/No formal Procedure

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P 3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Firewall Implementation** | F/ S | N | N | F/ H | N | F/ H | N | F/ H | F/ S | F/ S | F/ S F/ H | F/ H | F/ H | F/H | N | F/ S | F/ S | F/ S | F/ S |
| **Firewall Administration and Upgrade** | P | - | - | N | - | P | - | P | P | P | P | N | P | P (A) | - | P | P (A) | P | P (A) |
| **Service and Ports Blocking** | A | - | - | A | - | A | - | A | S | A | A | A | A | A | - | A | A | A | A |
| **Network Isolation mechanisms** | N | N | N | N | N | Y | Y | Y | Y | Y * | Y * | Y * | Y * | Y * | Y | Y * | Y * | Y * | Y * |

**Table H.1:** Firewall Implementation and Network Isolation



b.)Dialup Connectivity to Corporate Network **Y-** Yes **N-** No **R-** Restricted access/Secure connection **F-** Firewall isolation

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Use of direct dialup to Corporate Network** | Y | Y | Y | Y | Y | Y | N | N | N | N | Y | Y | Y | N | Y | - | Y | Y | Y |
| **access control to dialup** | * | * | * | * | * | * | * | * | * | * | R * | * | F | - | R * | * | * | * | R * |

**Table H.2:** Dialup Connectivity to Corporate Network * - Password authentication used

## II.) Network Equipment and Inter-Network Access

**Y –Yes** **N- No** **RP-** Regular and Procedure in Place

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Access Control Implementation in LAN** | Y | Y | N | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | Y | N | Y | N | Y | N |
| **Access Control Implementation in WAN** | Y | - | - | Y | - | - | Y | Y | Y | Y | Y | Y | Y | N | N | Y | Y | Y | Y |
| **Access Control Implementation in VPN /Etc...** | - | - | - | - | - | - | Y | - | Y | Y | - | - | - | - | - | Y | Y | Y | Y |
| | | | | | | | | | | | | | | | | | | | |
| **Maintenance of Passwords to routers and switches** | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| | | | | | | | | | | | | | | | | | | | |
| **Wireless Implementations** | N | N | N | N | N | Y | Y | N | Y | Y | Y | N | N | N | N | N | Y | Y | Y |
| **Security in Wireless implementations** | - | - | - | - | - | * | * | - | * | * | * | - | - | - | - | - | * | * | * |

**Table H.3:** Network Equipment and Network Access

* - No Special Security Mechanisms in placed / Passwords are used

# Annex -I

## IT Security for Corporate Users and Clients

### I.) Resource Allocation

**S – Satisfactory** **F- Fair** **ISP- Service provider Standards**
**R- Restricted** **N- No/ No restriction** **d- Unwanted Hardware disabled**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T 1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| User awareness on IT services Published | S | S | S | S | F | N | S | S | N | S | S | S | S | S | S | S | S | F | S |
| Acceptable and Non acceptable levels of resources they have granted | F | S | N | N | N | N | N | F | N | S | F | S | N | S | N | F | S | S | F |
| Application/Appliance usage | R | R | R | R | R | R | R | R | R | R | R | R | R | Less | R | R | R | R | Less |
| Pc locks | N | N | Y | Y | Y | N | Y d | Y | N | N | Y | Y | Y | Y | Y | Y | N | N | Y |
| Mailbox Limitations | R | R | R | R | R | N | R | R | R | N | R | R | R | R | R | R | | N | R |
| Shared drives Limitations | N | ISP - | ISP - | N | ISP - | N | N | ISP - | N | N | Y | N | Y | Y | Y (m) | N | | N | Y |

**Table I.1** : IT Resource Allocation

## II.) Authorization and Clearances

**Y – Yes** **N – No** **SLA – Service Agreements**

| | G1 | G2 | G3 | G4 | G5 | SG 1 | SG 2 | SG 3 | SG 4 | SG 5 | P1 | P2 | P3 | P4 | P5 | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Agreement Mechanism on Policy or standard** | N | Y (R) | N | N | N | N | Y (G) | N | Y (G) | N | Y (R) | Y (R) | N | Y (R) (G) | N | Y (R) | Y (R) | Y (R) | N |
| **User Level IT clearance** | Y | Y | N | N | N | Y | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | N |
| **Application level IT clearance** | Y | Y | N | N | N | N | Y | N | Y | N | Y | Y | N | Y | Y | Y | Y | N | Y |
| **External User Resource allocation** | - | - | - | - | - | SLA | SLA | - | - | | Y | - | - | - | - | - | - | - | - |
| **External User IT Clearance** | - | - | - | - | - | - | - | - | - | | Y | - | - | Y | Y | - | - | - | - |



**Table I.2:** Authorization and IT Clearance