**Supplement C  
TELECOMMUNICATIONS SERVICES QUESTIONNAIRE**

1. Please indicate all of the following services currently generating revenue for your organization:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Type** | **% of Prior Year Revenue** | **% of Current Annual Revenue** |
|  | 24 X 7 access to help desk, remote management,  network support services |  |  |
|  | 911 Services |  |  |
|  | Asset services (describe): |  |  |
|  | Call Centers – other (describe): |  |  |
|  | Call reception, logging and management |  |  |
|  | Data Centers: hosting, co-location, aggregation, etc. (describe): |  |  |
|  | Design, build, optimize secure, fixed and wireless networks |  |  |
|  | Engineering services to perform roll-outs, software and hardware upgrades, equipment moves and installation |  |  |
|  | Engineering services to provide warranty and maintenance support of major desktop systems, software and peripherals |  |  |
|  | Enterprise and personal computing solutions |  |  |
|  | Integration & logistic services |  |  |
|  | Internet protocol only |  |  |
|  | Internet telephony / VoIP |  |  |
|  | Local exchange services |  |  |
|  | Long distance |  |  |
|  | Managed maintenance of IT and non-IT environments |  |  |
|  | Public switched and internet protocol |  |  |
|  | Public switched telephone network only |  |  |
|  | Reseller, network (indicate switched or switchless and nature of service) |  |  |
|  | Satellite communications |  |  |
|  | Security: managed security, firewalls, filters, SPAM detection, etc.  Explain: |  |  |
|  | Single point of contact call management and problem resolution |  |  |
|  | Video/teleconferencing services |  |  |
|  | Virtual Private Networks |  |  |
|  | Wireless, indicate what:   |  | | --- | | 1. Beeper/pager 2. Cellular telephone communication carrier | | 1. Cellular telephone services | | 1. Microwave telecommunication resellers | | 1. Other wireless/radio, explain | | A.  B.  C.  D.  E. | A.  B.  C.  D.  E. |
|  | Other (describe): |  |  |
|  | **TOTAL** | **100%** | **100%** |

SECURITY & OPERATIONS

2. Who is responsible for data/network security within your firm?

Name:

Title:

|  |  | **YES** | **NO** |
| --- | --- | --- | --- |
|  | Are anti-virus tools and procedures used on desktops and mission critical servers? |  |  |
|  | Do you have a formal patch management process in place? |  |  |
|  | Do you receive CERT advisories or any other similar notification?  If yes, what action do you take as a result and what is the time frame for such action? |  |  |
|  | Do you state that your network is secure? |  |  |
|  | Do you authenticate remote users prior to allowing them to connect to private or dedicated lines, VPN’s,  computer systems, or internal networks? |  |  |
|  | Are all forms of Firewalls, SPAM Filters, Virus Protection and similar security measures updated at least quarterly? |  |  |
|  | Does your security system include password protection? |  |  |
|  | Do you have internal data security? |  |  |
|  | Do you store, manage, utilize, transmit or otherwise handle Personal Identifying Information (PII) such as Social Security Numbers, Credit Card Numbers, Bank Account Numbers, Health Records, etc for any of the following: Employees  Vendors  Customers  Other Third Parties  Approx. No. of records kept:  <5k  5-50k  50-100k  100-500k  >500k % specify |  |  |
|  | Do others rely on your network for directly generating revenue or taking customer orders? |  |  |
|  | Do you provide 911 services as part of your service offering?  If no, is this clearly outlined in your contract with your customers?  If yes, is this service outsourced to a third party?  Do you obtain certificates of insurance from the third party?  What is the minimum limit of liability required? $ |  |  |
|  | Are back-up and recovery procedures for all mission critical systems in place and documented? |  |  |
|  | Are business continuity plans in place for all mission critical business processes? |  |  |
|  | Are your network and computer systems monitored? |  |  |
|  | Do you outsource the management or maintenance of any part of your computer system or network, such as servers, firewalls, etc. to others?  If yes, please provide details of vendors, including their names and services provided: |  |  |
|  | Do you perform background checks, including credit and criminal history, on employees, independent consultants, and vendors? |  |  |
|  | Are all employees required to sign a statement that allows you to conduct mid-employment screenings at your discretion? |  |  |
|  | Are all employees provided with your systems security policy manual?  If yes, are they required to provide written confirmation acknowledging that they have read and understand the security policy? |  |  |
|  | Are employees required to sign a statement confirming that failure to follow security procedures as set forth in your systems security policy manual will result in disciplinary action that could include termination? |  |  |
|  | Do employee termination procedures include immediate revocation of all access to systems, facilities and  networks? |  |  |
|  | Have you experienced a physical, network or system security breach?  If yes, please provide details:    If Yes, What steps have you taken to prevent it from occurring again? |  |  |
|  | How do you learn about newly discovered weaknesses? | | |
|  | Describe firewalls used to prevent unauthorized access from computer systems and both internal & external networks? | | |
|  | Describe encryption used to secure data and information. | | |
|  | How often are the tools and procedures updated? | | |

**NETWORK - AVAILABILITY & REDUNDANCY**

1. Does your network redundancy and availability loss prevention include the following?

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **YES** | **NO** |
| a. | Looped network architecture |  |  |
| b. | Network monitoring with automatic response |  |  |
| c. | Load balancing available and offered to all customers |  |  |
| d. | Management of third party providers (audits, agreements, etc.) |  |  |
| e. | Dependency on third party networks |  |  |
| f. | Back-up power |  |  |
| g. | Automatic virus/SPAM detection operating over your entire network |  |  |
| h. | Do you use a standard service level agreement where parameters for network availability are clearly explained |  |  |

If none of the above referenced processes/procedures are used, please explain your approach to network redundancy and loss prevention:

## 

## 

**PHYSICAL PROTECTION**

1. Does your physical protection include the following?

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **YES** | **NO** |
| a. | Automatic sprinkler system connected to a central station alarm |  |  |
| b. | Automatic smoke detection connected to a central station alarm |  |  |
| c. | Automatic heat detection connected to a central station alarm |  |  |
| d. | Premises intrusion detection connected to a central station alarm |  |  |
| e. | Power surge protection |  |  |
| f. | Independent back-up power supply |  |  |
| g. | Emergency response team |  |  |
| h. | 100% hot site redundancy (back-up site) |  |  |

Electronic Signature of Authorized Representative: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:

Printed Name of Authorized Representative:       Title: