|  |  |  |  |
| --- | --- | --- | --- |
| **Project Name** | Operation Up-To-Date | Project Number | D0725 |
| **Project Manager** | Anthony Meunier | Prioritization | 1A |
| **Owner(s)** | Small Business Systems Inc. |

|  |  |
| --- | --- |
| **Statement of Work—Project Description and**  **Project Product** | *Operation Up-To-Date will provide a platform of small office networking equipment and set-up for Small Business Systems Inc. that will allow them to stay competitive and up-to-date in their field of business. By providing the company a high-tech, updated system of computers and related systems and then configuring all these systems to work in tandem with one another, Small Business Systems Inc. will be equipped with the tools necessary to provide its customers the best in efficient and caring service.*  *By recommendation of our Information Technology Analyst after his survey and research of the company, fifteen PCs will be acquired and installed in the offices of Small Business Systems Inc. Two server systems will also be secured and configured in order to achieve resource sharing, database management and overall provide a platform for interoperability and interconnectivity with the business’s systems. All required networking hardware and equipment will also be provided and installed in order to achieve a secure, dependable wired network of systems to ensure the fastest possible throughput in relation to the office’s current ISP-configuration. All systems will have the capacity to be shared and managed by an appointed local system administrator, and services can be configured such as printer, fax, scan, and copier sharing. In addition to the mentioned pieces of equipment, all-in-one printers containing all these functions will also be integrated into the office environment in order to maximize productivity while keeping clutter and excess costs to a minimum.*  *Our Systems Administrator expert will configure all devices in a manner that will allow them access to a shared database and resource-pool of data in order to provide the business with direct methods of conducting business and processing orders. These databases and all relevant data will be configured to work jointly with a 3rd party remote backup service that will provide real-time data backup of all internal systems. This provides a reliable and stable means of disaster protection and outfits the company with additional means of storage capacity. In addition, a secure Virtual Private Network System (VPN) system will be configured to work directly within the server system that provides both the function of secure, encrypted access to the Internet and all business activities conducting while online in addition to serving as a framework for remote connections to access the business server and its database from external locations.*  *Finally, an extensive security system of surveillance cameras will be purchased and configured to work within the networked system. This security system will be provided by a 3rd party company who specialize in providing surveillance solutions to businesses. Cameras will be secured and affixed to multiple outside locations around the facility and will be directly connected to each and every other networked device. This will provide multiple sources of monitoring when desired and will also take advantage of all storage space available in the network to save security feeds.*  *This project not only provides a stable and up-to-date platform for Small Business Systems Inc. to achieve business success immediately, but it also serves as a stepping stone for the company’s future as well because it lays the framework for any future additions to the system. In order for any business to be successful, you first need strong underlying values and principles that help solidify and help your business plan come to life – Operation Up-To-Date provides the technological values and principles that will help take Small Business Systems Inc. to the next level of success!* |
|  | |

|  |  |  |
| --- | --- | --- |
| **Project Deliverables** | 1. *Business requirements document including approved blueprint with layout of system hardware in accordance with employee position requirements* 2. *Desktop computer systems* 3. *Computer server devices* 4. *Network hardware, including routers and switches* 5. *Printers, Scanner, Fax, Copier and similar resource-shared equipment* 6. *Security cameras* 7. *Software relevant to setup of each hardware component* 8. *VPN implementation* 9. *Cloud data service* 10. *Support document detailing included technical support and troubleshooting* 11. *Network specifications including management tools such as passwords, etc.* | |
|  | | |
| **Project Objectives** | *The objective of this project is to develop and provide a modern computer network set-up to the main office of Small Business Systems Inc. This project will completely replace any current system in place and is set to be complete by February 26, 2015 at a budgeted cost of $85,000. The goals of the project include the following:*   * *Develop a completely new network of computer systems based on amount of users working at the company office* * *Provide and install framework to enable functionality of network, including switches, routers, and cabling required to connect equipment* * *Provide and install all required network hardware, including computer, server, and printing systems* * *Load and configure appropriate software on computer and server systems* * *Integrate security camera system into network and configure related software* * *Configure Virtual Private Network* * *Provide system to enable automated backup of data to remote server* * *Include lifetime technical support and troubleshooting of products and system installed* * *Reduce repair and maintenance costs by unifying systems and resources and eliminating redundancies* | |
| **Project Assumptions** | 1. *Security system will require minimal external factors and will tie in directly to network* 2. *Amount of networked devices will be easily controlled and operated by (two) server devices* 3. *Amount of networked devices will be achievable on fully wired system for best performance* 4. *Wireless functionality is not needed, but will be integrated for future expansion* 5. *There will be a user with sufficient technical knowledge to be system administrator* 6. *Pre-existing wiring is in stable shape and can contribute to new set-up* 7. *Storage size of backup files will be sufficient for company’s needs* 8. *Pre-existing internet connection is sufficient* 9. *Periods of network downtime are considered acceptable to company* 10. *Areas in need of highest security will be included in camera placement without hindrance due to natural or building obstructions* 11. *External temperatures will allow proper function of outside security equipment* 12. *All components in system will interconnect and function as intended* 13. *Employees using system already have basic Windows operating system skills* 14. *No physical internal security is necessary* 15. *All ordered equipment is promptly available and will not have any physical or operational defects* 16. *Any and all required legal documents/notices relating to surveillance equipment and set up are attained by company* | |
| **Project Constraints** | Amount of bandwidth received from Internet Service Provider (ISP)Quality of ISP’s physical equipment at location (i.e., degraded cable line)Data Protection Act, client data will only be kept for relevant purposes and not longer than necessary for those purposesMust adhere to laws about notification of being filmed via security camerasComputer and network employee usage policy is important because all resources are now shared and managedPasswords and user account levels implemented for both company and client protectionEncryption of data (such as VPN) must be lawful and compliant with any government restrictions for business dealingsSize of remote backup files may exceed limits of third parties; third parties may charge additional fees for this service  1. *Client budget ultimately dictates size, scope, and technicality of the project* 2. *Accessibility of building structure; factors such as crawl space, etc.* 3. *Building layout and wall thickness, in the event of any wireless systems implemented* 4. *Usable and relevant life cycle of software being installed* 5. *Preservation of surrounding community privacy could be questionable due to security cameras* | |
| **Exclusions** | 1. *Cannot account entirely for future growth and needs* 2. *Need to work within projected budget to provide services most needed now* 3. *Implementation of server device now does not necessarily hold processing power for any future devices* 4. *Physical security system can only be so in-depth while remaining under budget* 5. *More physical security cannot be added due to current space (i.e., server room or locked equipment); not necessary for only a small business* 6. *Technical support limitations; can only provide troubleshooting for devices we installed* 7. *No additional backup equipment at the moment; all done via Cloud* 8. *Integration for using outside devices, via VPN connection, lacking* 9. *Management of computer software security systems such as basic firewall and virus protection (will be managed by client)* 10. *External methods of processing client orders, like payment or fulfillment, will not be addressed* 11. *Functionality and capacity for future users* 12. *Environmental conditions of office where equipment will be stored; heat generated from large number of electronic systems* 13. *Cleanliness of systems or methods to manage/address key issues such as dust build up over time* | |
| **Acceptance Criteria** | *First and foremost, successful physical set-up of all required hardware is the basis for determining project success. Proper implementation of physical devices is key in connecting the systems as one, unified network. Software setup and configuration such as setting permissions and configuring sharing functions serve as the second point of emphasis. Implementing software security layers, such as the VPN, and then physical security by way of network-connected security devices serve as key elements in rounding out and completing the setup of the network. Finally, an offsite backup plan provides the final criteria for integration of all these devices and their successful set-up.*  *The end result of this project will provide products and services that better encompass the scope of business operations for Small Business Systems Inc. The products, which include computer systems, networking equipment, printers, servers, and all relevant software services will enable to company to perform all business activities in a capacity that meets and exceeds the standards set forth in the industry for providing fast and efficient order processing and delivery of goods and services.*  *The following criteria outline key functions of the project and determine project completion:*   * *Interconnected network of local office computers* * *Shared access to all network resources, including devices such as printers* * *Server functionality which allows for user authorization levels* * *Network-connected security system which can be controlled and monitored via local network* * *Security integration via use of added VPN network* * *Remote access to business network via VPN connection* * *Backup of company data to remote cloud server* | |
| |  |  | | --- | --- | | **Technical Requirements** | *In order to implement this project there must first be a thorough assessment of business requirements. From this assessment it can be determined how many systems are required in developing and connecting the network as a whole. Because the office houses 15 employees, all of whom need regular access to a computer system in order to access and process orders required to process and fulfill job requirements, it is imperative that each user is provided and maintains their own, unique computer system to conduct business on.*  *The goal of this project aside from physical assessment and setup of all required hardware is to develop and integrate a shared database of company-wide resources. In order to accomplish this, all computer and network systems will be connected to a pool of servers which can manage and distribute any and all necessary documents between each unique computer. Essentially, all users have the capacity to operate independently while also being able to tap into a shared network of documents and resources when desired.*  *The resource sharing of network components exists both at the physical and software levels. Firstly, (15) individual HP ProOne 600 G1 All-in-One PCs will be used in this network setup. These PCs provide the capacity for related products (primarily from the HP-line of enterprise computing products) to communicate with one another via a simple wired or wireless connection. Interfacing is done simultaneously across integrated network chipsets included on the motherboard that enables these devices to receive commands and processes from one another. This in itself addresses the notion of interconnected, shared network devices. However an external, centralized device is recommended to best manage and allocate traffic amongst these devices. Additionally, these All-in-One workstations serve as a cost-efficient method of outfitting the business capable business machines because the fact that they are all in one means no extra monitors are required to be purchased. Also, these systems can be bought directly from the manufacturer with no preloaded (Windows) software in bulk packages which saves on cost.*  *Expanding on that concept is the introduction of an HP ProLiant MicroServer Gen8 into the network system. For this size office, (3) HP ProLiant MicroServer Gen8’s will be added in order to provide sufficient processing power to allow the network to be self-sustaining and dependable under load. While these systems do come with HP-side software solutions to interconnect all the devices, its best left to only let the HP products interface with one another via the hardware chipset on the motherboards and use an external means of interfacing the hardware with each other from a user-level software solution.*  *Appropriate software makes integration and management of the systems a breeze. In this case, Windows is the preferred operating system due to user-experience and history. Therefore, (1) Windows Server 64-Bit will be installed on all hardware systems to provide a platform for cohesive user interaction and resource management. This operating system comes in various versions at multiple price points, but for this project a more expensive Enterprise edition will be used because there are no user limits or installation caps. This will allow only one copy of the product to be purchased and then be used to fulfill all 15 computers’ and 3 server devices’ software requirements. In addition, any future users or computer systems that are introduced in the company will theoretically have access to the same software platform as all existing computers, without the need for extra added cost down the line.*  *Windows Server will provide the required tools in the form of a domain to configure user accounts and designate an appropriate administrator-level user to manage the domain accounts. From this administrator account, functions can and will be configured to enable common network sharing functions such as printer and device sharing which is performed from within the administration settings available on Windows Server. Not only will this enable sharing potential amongst office devices and data, it will also provide the ability to restrict access of information where and when desired.*  *All of the devices mentioned have software-enabled (via HP chipset) wireless interfacing capability, so all additional network equipment will be wireless-compatible as well in order to enable this function if it is ever needed, perhaps due to company growth. For this set-up, though, all network equipment will be physically connected and wired. Although this is initially requires more set-up, the results are faster, more reliable transfer speeds.*  *To achieve a fully wired set-up, appropriate network cables must be integrated. For an office of this size, we will need an estimated 1,000 feet of Cat5E Network Ethernet Cable. The caveat is each device will need to be plugged in individually to its respective port on network equipment. To achieve this we can splice the bulk cable and use IDC junction blocks to essentially transform each section of spliced cable into an individual cable of appropriate length with like-ends on each side for proper connection.*  *The Ethernet cable will then be plugged from each one of the networked devices to their closest appropriate network hub. We will split the office in sections of three. Essentially five computers per section dictates that we use one network-hub per section, for a total of (3) network hubs. Cisco FastHub 400 Series serves as a good choice for these devices because they provide a cost-effective way to blend the features of performance, manageability, flexibility and redundancy. 10BaseT/100BaseTX uplink ports ensure that full bandwidth is received from the existing ISP modem (to parent hub), and then to all child hubs.*  *To go along with interconnectivity of all office-systems, there will also be shared use of printing, faxing, scanning, and copying devices. In order to help consolidate resources, (3) HP LaserJet Pro 400 MFP M425dn multifunction laser printers will be acquired and installed in this set-up. These devices, again, will be implemented into each “divided” section of the office – one per every five computer systems/users. These multifunction printers include faxing, scanning, and copying in addition to printing, which will help eliminate redundancy in devices within the office. They are also rated to print up to 50,000 pages per month which should be suitable for the business’s needs.*  *After the network hardware and software is configured and performing at maximum specifications, an additional layer of security will be added to the network by the set-up and use of a Virtual Private Network. To keep this as simple and cost and time effective as possible, an SSL (Secure Sockets Layer) encryption method VPN will be created locally on one of the server systems. This method of VPN is clientless and does not require a specific software to be configured on each machine that uses the VPN. This implementation is done via the Microsoft Config and Network Connections menus, and then the matching key/login information is simply entered into a web browser on the client computers which establishes the secure connection for the duration. Theoretically this VPN will also allow access to the network-server and all its data even via remote connection sources that successfully login using the SSL credentials. This will allow business to be conducted in locations outside of the physical office which can add exponential potential to business operations as a whole.*  *As a final layer of security, a fully network-integrated security camera system will be implemented on office property in order to protect all of the valuable resources now housed within the building. In order to achieve this, we will need to contract out some devices and labor from Axis Communications who specialize in providing security and surveillance systems. All cameras will be fixed and arranged on the exterior of the building, and in this case we will use (6) AXIS M1113-E Network Cameras. By using six devices we can have full coverage by affixing two cameras to each side of the front of the building, two cameras to each side of the rear of the building, and then one device per each side of the building. These cameras are unique and suitable for this set-up because they function by power over Ethernet, which can be plugged directly into our existing network system and each computer can then individually access the camera feeds.*  *The final point of emphasis in effective implementation and completion of this project is a remote backup system capable of storing all of the business’s data in a remote, off-site location. What this provides is a means of disaster-recovery in a worst case scenario. If any point/device in the network experiences a hardware malfunction which results in a complete loss, this backup system provides a platform where all the data is stored and can easily be attained via a downloadable system-clone for each unique computer. For this service, Carbonite will be purchased and installed for every PC on the network. What Carbonite specifically provides is real-time Cloud backup. When the software is run on a system, all files are sent to the Cloud automatically and continually. In addition, SSL encryption is once again used to ensure the safest file transfers, adding yet a final layer of security to round out the new network setup that Tech Fitters will provide during Operation Up-To-Date.* | | | |
|  | | |
| **APPROVALS** | | |
| Type Name | Signature | Date |
| Project Manager Approval | Anthony Meunier  Vice President of Systems Development  Tech Fitters, LLC | January 22, 2015 |
| **Customer or Sponsor Approval** | Dean Stanton  President, Small Business Systems Inc. | January 22, 2015 |