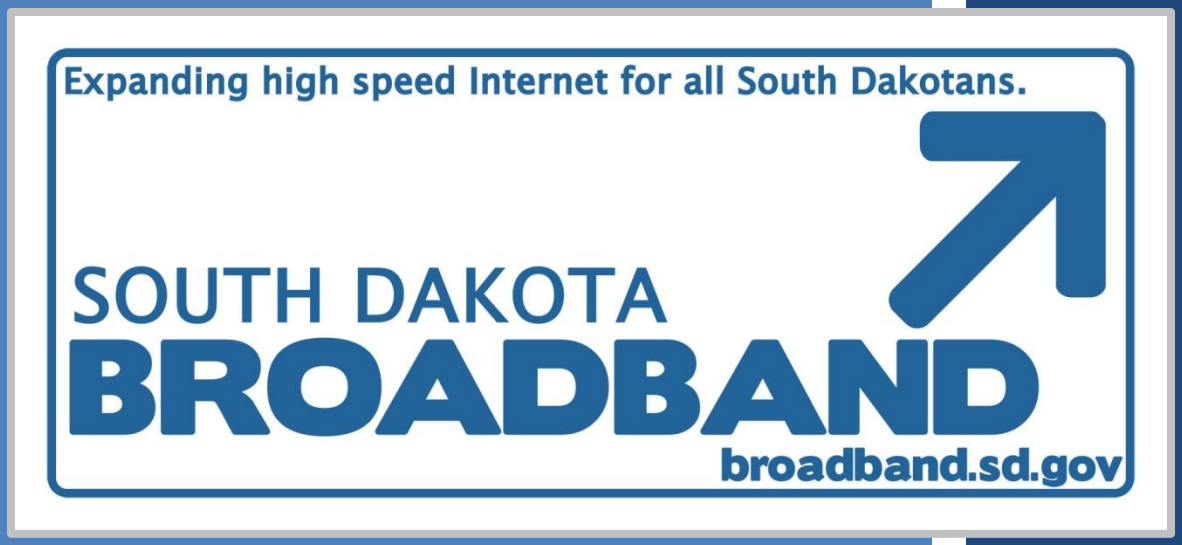

SOUTH DAKOTA BROADBAND INITIATIVE TECHNOLGY PLANNING ASSESSMENT

[Community Anchor Institution Name]
Community Anchor Institution Address

South Dakota Bureau of Information and Telecommunications (BIT)

700 Governors Drive
Pierre, SD 57501
605-773-4165

Contents

Overview 2

About the Institution 3

- Current Landscape 3
- Annual Technology Budget 3

Current Technologies 4

- Internet Service Provider 4
- Hardware Summary 4
- Specialized Applications 4
- Network Security and Threat Management 4
- Primary Issues, Needs and Objectives 5
- Current Status of Issues, Needs and Objectives 5
- Current Status of Additional Items 6

Future Technologies 7

- Cost Summary 7
- Additional Recommendations 8
- Thank You 8

Overview

The Baseline Technology Planning Assessment provides Community Anchor Institutions (CAI's) with a "snapshot" of their current technology environment. This snapshot gauges an institution's present technical posture and health. Through a process of delineation and consultation, we can address any issues they are currently experiencing that prohibit getting the full benefit of broadband services. This process also allows us to address any technologies that the Community Anchor Institution would like to implement, as well as our suggestions, to create a secure, managed computing environment. This ensures connection uptime, allowing users to get the full benefit of broadband related services. The primary areas to be assessed as they relate to the Community Anchor Institutions goals and intentions are:

- Broadband sufficiency, availability and continuity
- Current technical issues
- Technology management
- User best practices and procedures
- Risk mitigation and security
- Solution sustainability

This Technology Assessment summarizes the short and long term strategy for the Community Anchor Institution's technical infrastructure. Acting as a visual reference illustrating the findings of a needs analysis, the assessment also serves as a reference document for all involved parties, including local staff, contractors, service providers, and the South Dakota Broadband Technology Planning Team, to use as a guide in helping the institution achieve their technological goals and get the most of the broadband usage experience.

Network documentation is delivered to the Community Anchor Institution upon completion of the Technology Assessment. Included are diagrams of the present infrastructure as well as diagrams depicting the changes made after implementing technology upgrades and configurations.

At the time of the initial onsite Technology Assessment, the State Broadband Technology Planning Team will work to address any present issues. Some issues may require the involvement of other parties or involve longer term planning and purchasing actions. For these items, the Technology Planning Team will maintain communication with all necessary parties and assist wherever possible in seeing them through to completion. This includes any installations, reconfiguration and implementations of technological solutions.

At the completion of the implementations, a review is performed by the Technology Planning Team to evaluate the difference between the initial "snapshot" of the environment, the set technical objectives of the institution and the newly implemented technology resources and practices. The team will remain available for assistance for any ongoing items.

About the Institution

Current Landscape

The *[Community Anchor Institution Name]* is a public facility that houses 65 staff. The facility sees anywhere from 600 to 1,000+ clients on a daily basis. No primary technology coordinator is in place, as the size of the technical environment doesn't justify it. The main technical contact is the site administrator, *[Name]*. The staff of *[Community Anchor Institution Name]* would like to improve their technology posture through standardization and make some improvements with equipment updates. The following technical objectives are being requested by local staff:

- Increase speed and reliability of connectivity
- Update PC's
- Centralize file services
- Standardize PC operating systems and software

Upon our consultation with the *[Community Anchor Institution Name]*, the following objectives were added:

- Offer a public wifi hotspot
- Install a separate secure wifi network for staff
- Install a data backup solution
- Develop a disaster recovery plan
- Instigate desktop management
- Install standardized anti-virus software
- Implement a web content filtering system with client-tracking abilities

The institution itself doesn't require full-time technical staff; however the influx of past technical staff coming and going has created a challenge in gaining knowledge and making improvements of the existing network. The site has made good use of all working components, but could benefit from standardized equipment, software, user best practices and documentation.

Annual Technology Budget

Lifecycle management of existing hardware needs to be planned every three to five years. *[Community Anchor Institution Name]* recently had an evaluation of the computers they currently have. The plan/budget varies each year based on need.

Current Technologies

Internet Service Provider

- *[Name]*
- *[Connection Type]*
- *[Subscribed speed]*
- *[Actual Speeds]*
    - Test 1: Approximately 9:00 am - 15.25Mbps DL/4.79 Mbps UL
    - Test 2: Approximately 9:05 am - 27.63Mbps DL/4.82 Mbps UL
    - Test 3: Approximately 9:15 am - 27.83Mbps DL/4.92 Mbps UL

Hardware Summary

- Workstations
    - 10 total
    - Variety of makes, models and specs as well as a variety of Windows Operating Systems and Microsoft Office
- Network Equipment (See attached network diagram for present topology)
    - Cisco Catalyst 2950 – IOS version 12.1 (22)
    - Belkin SOHO wireless router (also acts as wireless access point)
    - NetGear RangeMax WPN 824 v2 (also acts as wireless access point)
    - DOCSIS 2.0 Cable Modem
    - Autonomous network for 2 workstations for city employee - connects back to city network via frame relay– separate from YMCA data network
        - Cisco 1721 router
        - Linksys 16 port Ethernet switch
- Servers
    - HP DL 360
- Video
    - Autonomous video network separate from data network for playing video clips, advertisements and announcements on a constant rotation

Specialized Applications

- [Application Name and Function]

Network Security and Threat Management

- There is minimum security. While users have individual logins and passwords, workstations are not locked when left unattended. At the time of the evaluation, not all computers had antivirus software. No perimeter network security system

is in place, and the wireless network used by staff and visitors alike is unsecured, presenting a vulnerability to sensitive data and information.

Primary Issues, Needs and Objectives

The following were identified:

1. The wireless network is shared amongst both staff computers and the general public.
2. No firewall solution
3. No content filtering solution
4. No user tracking
5. Network and Internet connectivity are intermittent
6. SOHO (Small Office Home Office) equipment in place where more robust equipment could be used
7. DOCSIS 2.0 modem is in place instead of DOCSIS 3.0
8. Antivirus software on workstations either is absent or non-standardized
9. No standardized operating system
10. Windows patches are not kept up to date
11. Workstations are left unattended, unlocked and logged in*

**Creates potential access to sensitive information hosted in local data applications or other by nefarious individuals intentionally, or public users unintentionally.*

Current Status of Issues, Needs and Objectives

1. Unsecured wireless network shared amongst public and staff computers
    - It was suggested that two logically separate wireless networks be created; one for staff machine and one for public access. This would be done by placing a firewall at the network perimeter. This would also allow them to allocate a specific amount of bandwidth for the public users, ensuring that the staff would always have adequate broadband connection to conduct business, regardless of public usage.
2. No firewall solution
    - The aforementioned firewall would accommodate this need
3. No content filtering solution
    - A content filtering solution is integrated into the aforementioned firewall. This would allow the *[Community Anchor Institution Name]* to block obvious malicious content like pornography, malware sites, peer to peer, etc. while preserving the openness of a public broadband access hotspot
4. No user tracking
    - The proposed firewall solution does have user tracking ability with the purchase of additional hardware. However, other services are being investigated that require less investment and eliminate the need for further premise equipment.

5. Intermittent network and internet connectivity
    - The NetGear router is the first network hop after the modem. This places SOHO equipment at the critical link of their Internet connection. The firmware on this device was updated to alleviate the connection issues. Also, the antiquity of the modem was a contributing factor. The ISP was called to replace the DOCSIS 2.0 modem with a new DOCSIS 3.0 modem. Reports from the *[Community Anchor Institution Name]* staff in days following the upgrades indicate the intermittent connection issues have subsided.
6. SOHO (Small Office Home Office) equipment in place where more robust equipment could be used
    - We proposed that the SOHO equipment be replaced with more robust equipment. This will handle the load placed on equipment, since this is such a high traffic environment. The following items were suggested for upgrades:
        - Replace the SOHO wireless routers with enterprise access points. Also use small switches, instead of the integrated switches in these devices.
7. DOCSIS 2.0 modem is in place instead of DOCSIS 3.0
8. The Internet Service Provider has since installed a DOCSIS 3.0 cable modem.
9. Antivirus software on workstations either is absent, or non-standardized
    - This will be part of the PC upgrade, software standardization process
10. No standardized operating system
    - This will be part of the PC upgrade, software standardization process
11. Windows patches are not kept up to date
    - We informed users on the importance of patching workstations, especially after Microsoft Tuesday's.
12. Workstations are left unattended, unlocked and logged in
    - Users all have unique logins; however we informed them of the importance of locking workstations when left unattended.

Current Status of Additional Items

13. Desktop management
    - The *[Community Anchor Institution Name]* would like to implement Group Policy for desktop management. This will require the creation of a domain. They mentioned that a local business had some servers that they were willing to part with. Servers can also be purchased through the South Dakota Broadband Initiative discount pricing.
14. Backup solution
    - With the domain and servers in place, local backups can be performed using integrated Windows Backup. This can be backed up to external hard drives.
15. Disaster recovery plan
    - We discussed the possibility of backing up off-site using a cloud based solution. This will ultimately depend on how crucial the centrally stored data is/can be.
16. Wireless-Open Public/Secured Private

- Currently, the *[Community Anchor Institution Name]* has two wireless access points. These are accessed by both public users and internal staff. The suggestion would be to place two access points for the business network, with one in the front office and one in the back room. Also, place two access points, one in the front lobby, and one in the commons area for public access. It is possible that a public one could also be used in the back of the building. The public access would be unsecured and the private network would be secured using WPA-PSK with a hidden SSID.

Future Technologies

The following is a breakdown of the equipment needed to facilitate the desired improvements, upgrades and changes. The manufacturer choices are discussed during the initial Technology Assessment using the State Broadband equipment discount list.

Cost Summary for Improvements, Upgrades and New Implementations

The following prices are listed to serve **only** as an indicator of cost. **This is not a quote**. Upon request, a quote can be obtained from the state contract equipment vendor(s) provisioned for the South Dakota Broadband Initiative.

Qty	Device name	SKU	Unit Price	Total Price
1	Fortigate 50b firewall bundle*	FG-50B-BDL-US	TBD	TBD
	Annual subscription renewal		TBD	
4	HP MSM430 Dual Radio 802.11n Access Point	J9650A	362.00	1,448.00
2	HP V1810-8G Switch	J9449A#ABA	137.00	274.00
4	Cisco Power Injector (optional)	AIR-PWRINJ4=	64.07	256.28
2	HP ML110 Server	Broadband ML110	1,369.48	2,738.96
10	WinSvrCAL SNGL LicSAPk MVL DvcCAL	R18-00129	27.35	273.50
2	WinSvrStd 2008R2 SNGL MVL	P73-05005	454.54	909.08
				5,899.82

**Please note that these costs do not include any additional data or electrical wiring that may be necessary*

Additional Recommendations

Maintaining good network documentation will provide tools for better planning, improved troubleshooting and reduced downtime. We are providing you with current and recommended network diagrams, as well as documentation which include login credentials and network addressing. Please store this in a secure location.

Physical security is equally important. All network equipment should be housed in as secure of a location as possible. Not only as a safeguard from people with malicious intent (theft, vandalism, etc.) but as a safeguard against accidents (liquid spills, knocked off counter, etc.)

Thank You!

The South Dakota Broadband Technology Planning Team enjoys helping Community Anchor Institutions like the *[Community Anchor Institution Name]* get the most out of broadband usage. It benefits your patrons, employees and day to day operations, and continually opens doors of possibility. As it was once said, "Like electricity a century ago, broadband is a foundation for economic growth, job creation, global competitiveness and a better way of life."

The integrity and soundness of your internal technical infrastructure is vital to getting the most out of broadband usage and the services it delivers. The collaboration of Community Anchor Institutions, their technical staff, Internet Service Providers and the State Broadband Technology Planning team is a relationship that we intend to maintain. Please consider this an open invitation to contact us at any time that we can assist you.

The South Dakota Broadband Technology Planning Team
700 Governors Drive
Pierre, SD 57501
(605) 773-4165
broadband@state.sd.us