

**The Extent to Which Sensitive Information is Secured by Institutions that Donate  
Computers to Educational Settings**

Ngoni Murandu

Thesis submitted to the  
College of Human Resources and Education  
At West Virginia University  
in partial fulfillment of the requirements for the  
Degree of  
Master of Arts  
In Technology Education

David L. McCrory, Ph.D., Chair

R. Neal Shambaugh, Ph.D.

Daniel Hartley, Ed.D.

Department of Advanced Educational Studies

Morgantown, West Virginia

## **Abstract**

### **The Extent to Which Sensitive Information is Secured by Institutions that Donate Computers to Educational Settings**

**By Ngoni Murandu**

The research in this study focused on the question of data security. The primary education community is the recipient of large numbers of surplus and used computers from government and Universities. This study reviewed the levels of risk associated with the procedures to sanitize disk media before computers are used by K-12 public schools. National surveys and a localized sample, provide data on the levels of awareness among academic administrations for the need to safeguard electronic data.

## DEDICATION

I dedicate this to my loving wife Iolanda. Iolanda stuck with me through the toughest 24 months of our lives. Iolanda, I drew my strength from yours.

## ACKNOWLEDGEMENTS

The completion of this degree could not have been possible without the mentoring and advice of my committee chair, Dr. David McCrory. Dr. McCrory's advice was like a lightning rod that kept me grounded in reality. Your many years of experience were so evident in our many counseling sessions and you steered me onto the correct path.

Dr. Shambaugh, who embraced my obsession with technology and channeled my energy into something relevant for technology education. Dr Shambaugh you gave me the confidence to tackle this thesis head-on in the manner that I did. The lectures I attended offered much more than academic knowledge you provided encouragement for life.

Dr. Dan Hartley, I think I can confidently say that ninety percent of all technology education students can relate with you. Interaction with Dr Hartley always leaves you feeling like academic success is very possible. Dr. Dan you make it look like the goal is always just within reach.

Carol Spiroff, I want to extend a very special thank you to my guardian angel. Carol you made sure I had all the right paperwork at all the right moments. Even though this was not required at all, your support was crucial to my success.

## **Table of Contents**

Abstract.....	..ii
Dedication.....	..iii
Acknowledgements.....	..iv
Table of Contents.....	..v
List of Figures.....	..vii
List of Tables.....	..viii
List of Appendices.....	..ix

## **Chapter 1**

Introduction.....	..2
Significance of Study.....	..6
Research Questions to be answered.....	..9
Definition of Terms.....	..11
Assumptions.....	..13
Limitations.....	..14

## **Chapter 2                    Review of Literature**

Introduction.....	..15
History of Surplus Computers in the Secondary Market.....	..16

## **Chapter 3**

Methodology.....	..34
Data Collections and Instrument details.....	..36

Statistical Treatment of Data.....	39
<b>Chapter 4</b>	
Results .....	40
Discussion.....	48
Conclusions.....	51
Recommendations .....	53
References.....	54
Appendices.....	59
Vita.....	62
Approval / Admin Page	

## List of Figures

Figure 1.....	38
---------------	----

## List of Tables

Table 1	Binary Data Represented in Switches/Alternatives.....	27
Table 2	US Department of Defense 5220.22-M Clearing and Sanitization Matrix..	31
Table 3	Website Survey of State Flagship Universities.....	37
Table 5	Presence of a website with administrative surplus information.....	37
Table 4	Data Collection of sampled computers in WVU inventory.....	41
Table 6	The distribution of intranet vs. internet based instructions.....	42
Table 7	Flagship institutions that advocate data sanitation.....	42
Table 8	Institutions that provide data sanitation instruction procedures .....	43
Table 9	Distribution of computers Sampled.....	44
Table 10	The age distribution of the computers sampled.....	45
Table 11	Original Source of Computers Sampled.....	45
Table 12	The amounts of data recovered on stored hard disks.....	46
Table 13	Types of data recovered from sampled computers.....	47
Table 14	The distribution of data by sensitivity of information recovered.....	47

List of Appendices

Appendix A. Data from Land Grant University survey ..... 59

Appendix B. Curriculum Vitae.....62

## Chapter 1

### *Introduction*

It all started with a wrong turn. In 1995 Democratic Senator Patty Murray got lost in the U.S senate building. The senator ended up in the senate basement where she found “rows and rows of computers”. The senator inquired and was informed that these were surplus computers and that the government no longer had a use for them (Hudson, 2001). Inspired by what she saw, Senator Murray immediately began writing legislation for what later became known as Executive Order 12999. The legislation mandated the distribution of government surplus computers to schools nationwide. One year after the passing of EO 12999, between 30,000 and 50,000 computers had been distributed to the education system (Glennan, T.K.Jr., Baer, W.S. Prunell, S., Farnsworth, G., & Schuyler, G., 1997). The significant problem is that five years after EO 12999, the first signs of a procedural oversight began to rear their ugly heads. The earliest sign of major procedural oversight was the data breach of sensitive data by the Department of Energy in 2001 (Micek, 2001). An audit conducted by the office of the inspector general OIG at the Rocky Flats Environmental Technology Site, a nuclear research facility, found that computers had been sent to surplus without the clearing of “Unclassified Controlled Nuclear Information”. This study will examine the reports that followed and preceded these incidents in an effort to examine if there is a true risk to the nation and educational community in the documented methods of computer distribution. In addition to the factual study, a brief quantitative review will sample how a local environment like West Virginia University is aware of the potential risks and what measures have been taken to ensure that no sensitive data ends up in the public hands.

## *Background*

In order to function well, a desktop computer must have a hard disk drive. Almost all desktop computers that are used in the various departments in the federal government use hard disk drives. “These billions of hard disks do one thing well -- they store changing digital information in a relatively permanent form. They give computers the ability to remember things when the power goes out.” (HowStuffWorks, 2003).

Invented in the 1950s, hard disks started as large disks up to 20 inches in diameter holding just a few megabytes storage “the magnetic medium can be easily erased and rewritten, and it will "remember" the magnetic flux patterns stored onto the medium for many years.” (HowStuffWorks, 2003) .This bears implications for the departments that handle the surplus computer procedures for the many government organizations and educational institutions that donate computers to the educational arena.

In February of 2003, in Frankfort Kentucky, a state computer that had been marked for sale as surplus equipment contained confidential files identifying thousands of people with sexually transmitted diseases, including AIDS. (Wolfe,2003). In April of 2001, in an audit by the congressional General Accounting Office (GAO), it was found that the DOE does not have standardized procedures to train its own employees or the independent contractors who remove sensitive information from the agency's computers. In fact, during a random audit in Germantown Maryland, computers marked for surplus were found with sensitive information still on them. “The agency's computers store vast amounts of critical information, such as personal information about DOE employees, sensitive scientific and technical information, information about nuclear programs, and financial and budget documents, the GAO said,” (Micek ,2001) These are but a few examples that demonstrate the nature of the potential

problem that data poses for the process of donating surplus assets. The problem is that we have many anecdotal examples of significant breaches of data privacy through the surplus disposal process, but there are no academic studies that can report if this is a crisis that needs addressed or not. The legal liability that improper asset disposal represents, makes a study to assess the levels of these incidents an academic imperative. Simply tagging a computer as ready for surplus and then selling it or passing it onto public schools could result in the exposure of students to information about their community and institutions that should not have been released. Looking at the problem with a research approach may help provide answers as to whether or not data disposal is being taken seriously by the custodians of assets being handed down. The research problem focuses on the fact that this is a very new area of study. Desktop computers are only in their fourth generational cycle. This means that there have only been four significant points where inventory cycles would have resulted in large numbers of computers being sent to surplus or auction. These are related to the jumps in PC speed, when computers went from 486 MHz speed to 500 MHz Pentium speed and also when we moved from the 500 MHz to breaking the 1GHz barrier. Technology shifts result in massive “hand down” operations and the problem is scientifically assessing just how much data is lost during this process.

It may be difficult to assess just how much data exactly ends up in the secondary market, however it may be practical to assess the level of risk as a factor of the numbers of hard disks that are released without precautionary measures having been taken. If the numbers are high and the originators of the resources are known to handle potentially sensitive materials, then the possibility of significant risks being present in the market become elevated. Over the last six years, 1997-2003, the storage capacity of computer hard disks has increased. The impact

of this improvement in storage capacity meant that greater amounts of data could now be stored on computers. A computer in the department of social work, for example, could now be dedicated as a “file server”. This would be a computer with the sole purpose of warehousing large amounts of patient related data and case load reports. Such computers are now six years old and that is “old” in computer terms so the logical step would be to surplus such a computer. The problem is that without adequate data security procedures at the point when officials follow the requirements of EO12999 and sent these to schools, all that data goes to the school system along with the computer.

Once in the school systems, the computers that have been sent to the school systems with data are kept intact. This was initially because the computers that were donated were often left that way to provide the schools with a functioning operating system. In many cases well meaning officials admitted to having made the error of leaving data on computers because their intention was to pass on a working operating system. Operating system software is an expensive component of a computer system. Without it the computer does not work and often schools have to spend a large amount of money to furnish bare computers with one. Attempting to avoid this expense often involves the risk of an individual browsing the data directories on a hard disk for sensitive information which is where human error results. Data in these cases is often omitted and left for discovery by minors or public school officials who may not report these cases for fear of “biting the hand that feeds them”.

### *Significance of Study*

This study is designed to assess the current practice with respect to the preventative measures that are being employed by organizations whose computers often end up in secondary markets.

The purpose of the assessment is to provide baseline data on whether unsecured data is indeed a risk to the public education system. Data derived from this will assist in the determination of the level of liability that donating institutions open themselves up to when passing on computers with data still on them. There have been significant protections introduced as legislation to protect the privacy of individuals who interact with health and commercial enterprises. During the course of regular business activities these institutions take great precautions to ensure client and participant privacy but there is a potential issue at disposal. This study will evaluate representative samples and attempt to generalize the results to see if there is a problem with data being lost at disposal of computer hardware. On April 14<sup>th</sup> 2003, the Health Insurance Privacy and Accountability Act HIPAA was enforced into action (HIPAA, 1996). The act, which covers how medical information relating to human subjects is treated, covers data stored on disk drives. The precaution in the HIPAA statute that covers data states

“media controls would be required in the form of formal, documented policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility. They are important to ensure total control of media containing health information. These controls would include the following mandatory implementation features: Controlled access to media, Accountability

(tracking mechanism), Data backup, data storage and disposal.” (Centers for Medicare & Medicaid Services, 2003).

This clearly places responsibility for the secured disposal of computer hard disks in the hands of institutions that directly donate computers to the educational arena. The philanthropic act of passing on computers has been proceeding at full speed, yet we do not have a current assessment of the measures taken to ensure secure disk cleanings. Where measures to erase information on hard disks have taken place it is also critical that an academic study examines the effectiveness of these methods employed. It is a logical inference to assume that in some cases there may be cases of ineffective methods of data disposal and security. In terms of institutional liability, health related data breach penalties are fairly extensive. HIPAA mandates that for a breach of security, intentional or unintentional fines may rise as high as \$250,000 (HIPAA, SEC. 1177, 1996). This is only the financial federal penalty; the breach of data related to patient information may also be subject to criminal prosecution with a sentence of up to twenty five years in jail and civil judgments. The motivation certainly exists for the tertiary educational institution and the donating corporation to consider the gravity of the issue. This study will investigate and assess the level of trepidation and precaution that custodians of computers scheduled for surplus deal with when they are planning to dispose of computers. There is also a significant need to examine the general consensus in accepted methods of secure data disposal. Many experts in computer media security recommend many different ways to effectively destroy data. This study examined the available methods of data disposal that would be practical for application by high volume donors like Universities and government departments. Certain methods of absolute data destruction involve measures that are time intensive, making the

process impractical for donors like the Senate in 1996 which donated thousands of computers to the educational consumers (Hudson, 2001).

Civil liability also exposes donors to consumers who may look at data retrieval as an opportunity to intentionally sue for financial gain. The current software market now provides consumers with a number of tools that provide the ability to probe hard drives that may have been cleaned with low impact methods. The information that these retrieval efforts obtain could be used in legal suits. Research can determine if the large numbers of computers that have been sent down to public schools and libraries now pose this potential high risk. This study took a representative scenario and attempt to set the base for an extrapolation and generalization to these relevant areas.

The final consideration is one of precautionary measures for the sake of the student recipients of these computers. In cases where the cases are violated there may be information that is highly inappropriate for minors or generally offensive on these computers. This could potentially result in embarrassing situations for the donors of computers or worse if civil rights are abused.

The study also examined the effects of a new trend in precautionary measures. The trend involves donors passing on computers without the hard drives in the computers and opting to recycle the hard disks internally. This adds an additional burden to the recipients of these donations and may slow down the pace of computer integration in public school classrooms.

### *The Research Questions*

There are several research questions that required answers. The questions are listed as follows:

1. Are the recipients of surplus computers currently also the recipients of sensitive and inappropriate data?

The recipients of surplus computers focused in this study are public schools and after-school programs. These institutions are often involved in programs that are linked to EO 12959. Government and tertiary institutions have many reasons for donating assets to these schools, such as community development and outreach. The fact that the computers from federal departments end up in schools is established through documented accounts, however research needs to establish whether as a part of the hand down process, computers are being donated with sensitive data still intact and transmittable on these computers.

2. What are the risks of the information to educational recipients such as K-12 schools and what steps should be taken?

The original uses of these computers vary depending on the initial roles the donor agency play in society. Computers from the office of geographical studies at West Virginia University probably bear a lower security risk than those that are donated to public schools by DARPA. The questions that the research will investigate will focus on the numbers involved and attempt to review if the numbers of computers from the various areas indicate a pattern that may show a level of risk for data loss from high security areas. The risk assessment will require an initial attempt at a remedy or at least a

recommendation of remedies. These possible solutions are limited by the need for practical considerations. The study will evaluate the effective methods of data destruction, looking at the level of effectiveness and the ability to proliferate these solutions on the scale required to ensure the continuity of computer based surplus programs.

3. Has the complexity of proper disposal procedures resulted in sensitive data being handed down to public schools and other programs?

Some departments and colleges have posted specific programs for the proper destruction of surplus data. These methods of data destruction vary in complexity. The levels of complexity in carrying out data disposal may be a factor in some data breaches. It may be significant for the study of these procedures to be analyzed for the impact that training and understanding on the part of the custodians may have in instances of information breaches. There are different methods of effectively deleting data permanently, however many of these involve using software that addresses the data clusters on the hard disks. These applications may be difficult to understand for the typical inventory clerk, who in most cases is the last person to oversee the disposal of assets destined for the educational platforms. The study aims to review the different types of posted instructions on the websites of Universities that document surplus procedures and examine the level of detail in the documented procedures. This level of detail may provide insight on how the procedures may need to be supplemented by training programs or any remedies that may address this issue and prevent more data breaches to the public communities.

### *Definitions of Terms*

**Sensitive Data** – Information that was generated as a part of the business or academic processes of the university that relates to data about individuals or groups who would not wish their information released.

**Hard Drive** - Computer based media storage. The primary computer storage device, which spins, reads and writes one or more fixed disk platters. In practice, the terms "hard drive" and "hard disk" are used synonymously. Hard drives are the storage medium in desktop and laptop computers as well as all servers and mainframes throughout the world. They are also used in printers for storing fonts and print jobs as well as MP3 players and a myriad of other portable and stationary computer-based devices. Although removable disks encased in cartridges use the same "hard" disk media and a similar drive technology, they are mostly called "removable drives" rather than hard drives. The term "hard" differentiates high-capacity rigid disks made of aluminum or glass from low-capacity floppy disks made of plastic (Techweb Encyclopedia, 2003).

**Surplus Computers**- These are computers that were purchased for use by University and or Federal departments that have been set aside or replaced by upgrades. Often these computers are placed in storage facilities for ultimate auction or donation to the K-12 market.

**Secondary Market**- Educational recipients of computer materials purchased or donated from Tertiary or Federal surplus stores.

**Donors**- The term donors for purposes of this study refers to Federal departments, Colleges and Universities, and private corporations that have established programs to pass on their used computers to public schools and other K-12 programs.

HIPAA - Health Insurance Portability and Accountability Act of 1996 (HIPAA): A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. Also known as the Kennedy-Kassebaum Bill, the Kassebaum-Kennedy Bill, K2, or Public Law 104-191, ( Public Law 104-191, 2003).

Desktop Computer- A single-user computer. Typically refers to a PC or Mac, but may also refer to a workstation from Sun, IBM, etc. Also called a "client computer" or "client." The term implies stationary use in contrast to a laptop, which is portable. (Techweb Encyclopedia, 2003)

CPU- (Central Processing Unit) The computing part of the computer. Also called the "processor," it is made up of the control unit and ALU. Today, the CPUs of almost all computers are contained on a single chipset. The CPU, clock and main memory make up a computer. A complete computer system requires the addition of control units, input, output and storage devices and an operating system. (Techweb Encyclopedia, 2003)

### *Assumptions*

The investigator assumed:

- Each Desktop Computer studied was intentionally set aside for surplus by the administration/ former custodians of the computer.
- The computers sampled from the Surplus repositories all have relatively equal opportunities of ending up in the public school system through donation and auction programs.
- The responses from participants will differ due to the varying perceptions of individuals and the varying procedures for the treatment of surplus data at each institution.
- The inventory statistics obtained from University of West Virginia records are accurate and reflect numbers accurate as indications of computers sent to surplus.
- Academic and Health related data found on WVU computers is regarded as Intellectual Property and still remains in the ownership of West Virginia University.
- The computers that have been deemed ready for auction/donation at WVU are not subject to any previous documented studies on follow up breached data.

### *Limitations*

- Data retrieval were limited to Win32, Mac and Unix platforms only . Computers that are sent to surplus from Mainframes and other unique operating systems were not included in the study.
- The computers in the population sample, while tagged for surplus, had not actually left WVU premises and thus remain in the custody of the University until auction /donation.
- Computers examined were limited to functioning disk drives. Drives that were damaged were not repaired nor were attempts to repair them for the purposes of data retrieval made.
- The procedures posted online by peer institutions may not be up to date and reflective of their actual procedures for surplus computers.

## Chapter 2

### *Review of Literature*

#### *Introduction*

The process of donating equipment to k-12 schools is not a new one. This has been a standard practice for many years. The advent of computers and the advantages they bring to the classroom have made their use a priority for many teachers. The benefits of computers in the classroom have been examined by many experts in the field of technology education and general education. There is significant literature which this study will shed light on, to demonstrate that the introductions of computers into school curriculum can contribute in great strides to student achievement.

The problem has been that once it was established that the computers benefited the classroom the market prices for computers did not lower over time to levels that the school budgets could afford them. This was particularly true in the 1990's when the technology was changing at a "lightning fast" pace. It appeared that during the technology boom of the nineties higher education institutions could afford to use their profits from market based endowments and recycled their computer assets or expanded capital purchases to levels that perpetuated large donations at the end of the decade as these computers got older.

Literature analyzing the process of donating surplus computers is very limited, and even fewer numbers of articles deal with the data loss as a result of improper disposal. The sources of information on incidents of data breaches will focus on the documentation of data being found by regulators in audits and then reported through the media in the form of print, television and web articles.

*History of Surplus computers in the Secondary Market.*

Researchers at Carnegie Mellon University estimate that the ratio of computers that are obsolete to those that are newly purchased is increasing. The ratio was initially 2:3 in the late 90's but by 2005 the ratio is predicted to be 1:1 (Starks, 2003). President Clinton signed Executive Order 12999 on April 17, 1996. The "Educational Technology: Ensuring Opportunity for All Children in the Next Century. EO 1299" was the first act to directly address the passing on of Federal computer assets to the education system, but it was not the first act to deal with the government's attempts to get technology in the classroom. There have been many initiatives to get computing technology in the hands of teachers. The General Services Administration (GSA) was officially created in June 1949. The service was activated with the enactment of the Federal Property and Administrative Services Act of 1949 (known as the Property Act). "The act was designed, in part, to increase the efficiency and economy of Federal government operations with regard to the procurement, utilization and disposal of property." (Office of Property disposal, 2003). Over the last fifty years portions of GSA have been amended by many pieces of legislation. Under the property act, materials once properly classified could be auctioned to the general public or sent to public schools. By the time that computers became disposable assets, procedures for their use in the public school systems were in place. The government provided motivation for private industry to get on the bandwagon of donating surplus technology to the educational system through the Stevenson-Wydler Technology Innovation Act of 1980, PL 96-480. The Act mandates Federal Laboratories to actively seek collaborative research with State and local governments, academia, nonprofit organizations or private industry. The federal government, under provisions of this act, disseminates information and established the Center for the

Utilization of Federal Technology at the National Technical Information Service. It is through this service that the availability and distribution of large computer asset stores can be coordinated. This legislation also established the National Medal of Technology. This medal, awarded by the President, is bestowed to either individuals or companies for "outstanding contributions to the promotion of technology or technological manpower for the improvement of the economic, environmental, or social well-being of the United States." (The Stevenson-Wydler Technology Innovation Agreement, 1980).

EO 12999 is the most comprehensive piece of legislation that addresses the distribution of assets to public schools. In section one of the Executive Order which reads

“Protection of Educationally Useful Federal Equipment. (a) Educationally useful Federal equipment is a vital national resource. To the extent such equipment can be used as is, separated into parts for other computers, or upgraded--either by professional technicians, students, or other recycling efforts--educationally useful Federal equipment is a valuable tool for computer education. Therefore, to the extent possible, all executive departments and agencies (hereinafter referred to as "agencies") shall protect and safeguard such equipment, particularly when declared excess or surplus, so that it may be recycled and transferred, if appropriate, pursuant to this order. This makes it clear to members of the federal agencies that the public schools take precedence in the planning and distribution of these assets. This point is even further clarified in section (b) of the order which states that “Agencies shall attempt to give particular preference to schools and nonprofit organizations.”

The problem in the perception of some commentators on the issue of data breaches is that the Executive Order also encouraged the distribution of “Educationally Useful” computers in

working condition. This is in the third section of the order c) "Educationally useful Federal equipment" means computers and related peripheral tools (e.g., printers, modems, routers, and servers), including telecommunications and research equipment, that are appropriate for use in pre-kindergarten, elementary, middle, or secondary school education." (Office of the Press Secretary, EO 12999). The computer data component referred in the section of that order states that educationally useful equipment shall also include computer software, where the transfer of licenses is permitted.

In order to qualify for computers donated under the EO 12999 system, eligible recipients must submit a letter of interest in order to obtain excess computer equipment from the department or agency that has announced the availability of assets. The letter must be on letterhead and signed by a senior authorizing official. The school or organization is required to designate a person or persons authorized to sign the SF-122, Transfer Order, on behalf of the eligible recipients. Schools are also asked to identify needed equipment in general terms. The school must certify that the requestor is qualified to receive property as an eligible school, school district, or community-based educational organization as defined in the EO 12999. Universities have their own unique procedures for local school boards to apply for eligibility to receive their used computers. The net result of all these stipulations is a great amount of "red tape" that schools have to overcome in order to get assets from donors. Despite the difficulty in obtaining surplus assets many public school teachers still actively pursue technology for incorporation in their classes. Understanding this drive may help in determining why these potential recipients of sensitive data may not be inclined to report data breaches. The value that public school educators place on computers in the classroom may

play a role in understanding the symbiotic relationship that they share with the donors of computer assets.

Educators in the public school system have documented the effects of computers in the classroom. Researchers like Kathleen Vail, note that “most states and districts have technology plans and teachers are being trained to integrate technology into their daily classroom lives. (Vail, 2003). This is supported by reports from the Heritage Foundation that an explosion in technology has increased efforts to equip every classroom with computers and "wire" every school to the Internet. The Heritage Foundation estimates that between September 1984 and September 1997 alone, the number of computers in America's K-12 schools increased eleven fold to more than 8 million units. The majority of these units are grant funded new purchases but a significant number of computers also come from recycled computer programs (Johnson, 2000). Studies have been conducted that have examined if the effect of computers in the classroom positively influences academic achievement. In 1997, the Educational Testing Service, collaborated with the National Center for Education Statistics and published a major study on computers and academic achievement. The researchers led by Dr. Harold Wenglinsky, used data from the 1996 National Assessment of Educational Progress math examination. The researchers analyzed student computer used both in class and at home. Their study generally showed a positive reaction to the technology. This type of academic feedback encourages educators to seek out programs that provide computers from the classroom. In addition to the NEAP study research is now available on the effects of the internet on classroom resources and information availability. This was evaluated by a research project conducted by SRI international in 1999. The project was a part of the Goal 2000 Technology and Education Reform project. The researchers

found that teachers from 10 out of 17 classrooms studied in great detail reported increased use of external resources as a benefit of using technology. (US Department of Education, 1995).

Further evidence that teachers were willing recipients of technology in the classroom up to early 2000 is seen in the work of Dr. Henry Jay Becker, a professor of education at the University of California, Irvine. Through the use of Surveys and field research, Becker showed “increases in learning when students used the computer to enhance sophisticated writing and complex reasoning activities” (Salpeter, 1998). Becker concluded that educators shift their focus from teaching individual technology skills and instead “include more constructivist learning opportunities in order to take full advantage of the technology” (Kimble, 1999). Additional backing to the pro technology bandwagon was provided by Larry Cuban, a professor at Stanford University. Dr Cuban has studied the impact of computers in classrooms (Salpeter, 1998). His conclusions were that drill and tutorial software positively impact student learning.

It must be noted that not all educational researchers have been in favor of the trend toward computers in the classroom. While their voices may be drowned by the stampede toward technology, educators like Dr Jane Healey voiced a number of concerns in her book, *Failure to Connect* (Healey, 1998). Dr Healy questioned if “unlimited access to computers in early primary years at the expense of more concrete learning experiences is helping or harming the development of children.” (Healy, 1998). Healy questioned the mindless drive toward outfitting classrooms with technology without any consideration to the curriculum and learning strategies that would need to adapt along with these changes.

Despite the varying literature, the drive toward computers in the classrooms is self evident. The EO 12959 impact study by Thomas K. Glennan, Jr., Walter S. Baer, Susanna Purnell, and Gwendolyn Farnsworth estimated that over 500,000 computers are eligible for transfer to the public school system under the government's disposal numbers. They estimate that at twenty percent of these approximately 100,000 computers are available for donation in full working condition. (Glennan, T.K.Jr., Baer, W.S. Prunell, S., Farnsworth, G., & Schuyler, G. 1997). With numbers so high the probability of sensitive data being passed on becomes extremely high. It is thus no surprise that there are many "incident reports" of data breaches involving computers from donor institutions.

The reports vary in gravity, In January of 2000; the U.S. Department of Energy's inspector general launched the inquiry at the request of Senator Thurmond, R-S.C. The Senator has received reports of surplus SRS computers containing secret data being tagged for sale, some to private companies in China, (Haddock, 2000). The investigation yielded that only one computer was found to have been actually shipped to China with sensitive data at the time the investigation was launched. A year later in April of 2001, despite having rules requiring it, officials at the U.S. Department of Energy (DOE) do not have clear procedures for purging sensitive information from computers. A report, released by the congressional General Accounting Office (GAO), also found that the DOE lacked standardized procedures to train its own employees or the contractors that remove sensitive data from the agency's computers. GAO auditors asserted that "DOE also does not ensure that procedures used to remove all software, information, and data from systems are effective,"(Micek, 2001). This apparent weakness in standardized procedures resulted in retrieval of sensitive data in fifty percent of all computers tested at 10 field offices of the department of energy by the General

Accounting office. In May of 2002 , Indianapolis WISH-TV, Channel 8, bought three personal computers sold as surplus by the local medical center. The computer hard drives contained Protected Health Information (PHI) and purchase card information that had not been deleted prior to disposal. As a result of the expose the medical center had to review the training and practices regarding disposal of surplus computers. The local authorities had to search out the people/organizations to which 139 computers were already donated or sold with data still possibly resident. These parties included educational institutions, the State of Indiana, and individual purchasers. (WISHTV-8, 2002)

Chris Dixon an investigative journalist who has reported actual incidents of data breach in the state of Pennsylvania. The computers in question were auctioned to the public by the Pennsylvania Department of General Services. The computers were found to contain social security numbers and employee salaries. This report was filed in March of 2002 which indicates that as the numbers of computers available to the secondary market increase the data dilemma will increase in its importance to overall public privacy and security. (Dixon, 2002).

In January 2003 MIT reported that two of its graduate students had uncovered “mountains of private data” on discarded hard drives. The study involved purchasing the hard disks from computers that had been made available to online auction sites. The study covered over 158 disk drives of which 129 were fully functional. The study highlighted the lack of appreciation for the value of data on computer hard drives by the custodians and owners of older computers that had been replaced by newer upgrades (TechTalk, 2003).

### *Universities Tackle the Risks*

Articles on the risks of data to secondary users have been written by Peter Hart from the University of Pittsburg. Dr. Hart wrote a piece on the appropriate method of disposal for computers that leave the inventory registers of the University of Pittsburg (Hart, 2003). The state of Arkansas has a state law that governs the practices of its state colleges with respect to surplus hard disks. The extract from the state legislation reads:

“The State of Arkansas, Act 1410, Section 4. (a)(2) mandates that "all hard drives of surplus computer equipment be degaussed, cleared of all data, software, and be otherwise prepared for sale within (90) days after replacement." Each department on campus is required to meet these sanitation guidelines for all surplus hard drives. The UA Surplus Warehouse department has been instructed to refuse any computer that is not sanitation certified. To ensure compliance, a new campus-wide procedure is effective immediate.” (Senate Bill 807, 2001).

This demonstrates an example of a clear attempt on the part of Arkansas legislators to recognize the risks posed by the potential liability derived from data breaches. This approach is similar to other colleges and Universities in another respect, the University of Arkansas displays its disposal procedures on the University website for use by all departments that surplus assets. Certain Universities like the University of Nebraska at Lincoln, post their requirements and procedures on line but the postings are brief and may pose potential training or implementation issues. Nebraska’s notice states: “Usable computer hardware that has been tagged as surplus equipment is reconditioned, including the replacement of defective parts and components and the re-formatting of hard drives, before being reallocated. Departments that elect to keep replaced computers that were purchased from department generated funds can request to have the hard drives reformatted.”(University of

Nebraska-Lincoln, 2003). The disposal procedures posting at Southwest Mississippi Community College (SMCC, 2003) does not address the issue of data destruction at all. Arizona State provides an elaborate checklist that covers all points from inventory checkouts to categorization, but it too neglects to inform the departments to destroy data from the hard disks before proceeding with disposition.

### *Pressure from Donors on Educators*

The motivation for private corporations to dispose of computers that they no longer use onto public schools may be multi faceted. A March 2001 article by Beth Wade, Managing editor of American City and County, highlights the disposal quandary that corporations face when looking to offload their surplus computers. Wade reports that the national safety Council had estimated that by 2006 over 500 million of the PCs in the US would become obsolete (Wade, 2001). Computer diversion programs are being sponsored by corporations as alternatives to landfills, Wade states. Landfills are solid waste areas where local ordinances have allowed a contractor to bury used equipment including computers into the earth. The practice of using landfills for computer disposals has resulted in a backlash for corporations that contracted to have their surplus computers disposed in this manner. The National Safety Council's Environmental Health Center, estimates only 11 percent of old personal computers are recycled. At this rate the problem of toxic computer landfill is expected to increase (Quain, 2002). According to the Environmental protection agency it costs an estimated \$25 to \$50 per computer to safely recycle surplus computers. This would mean that of the 325 million PCs that will become obsolete between 2002 and 2004 the cost of eco friendly disposal would be an estimated \$16 billion (Eastwood, 2002). The government allows companies to

export 80% of the waste but international laws make this increasingly difficult. International mandates like the Basel Convention in 1992, prohibit hazardous waste exports to underdeveloped nations (Eastwood, 2002).

A typical desktop computer is built with, materials that include: Plastics, Lead, Aluminum, Germanium, Gallium, Iron, Tin, Copper, Barium, Nickel, Zinc, Tantalum, Indium, Vanadium, Terbium, Beryllium, Gold, Europium, Titanium, Ruthenium, Cobalt, Palladium, Manganese, Silver, Antimony, Bismuth, Chromium, Cadmium, Selenium, Niobium, Yttrium, Rhodium, Platinum, Mercury, Arsenic, and Silica (Wood, 2003). The materials can have serious effects on human health. Each mineral has a different effect on human health. Lead which is located in cathode-ray tubes; solders of computer monitors contain five pounds of lead per tube. Lead poisoning may cause “damage to the central and peripheral nervous systems, blood system and kidneys in humans.” There have also been reports of damage to a child's brain development. (Wood, 2003)

The printed circuit boards and semiconductors contain cadmium. Cadmium compounds collect in the body, in particular in kidneys. Mercury, which causes brain damage, is contained in the batteries and switches. More recent designs of computer cases feature Chromium as corrosion protection in steel components. Wood estimates that By 2005, estimated 1.2 million pounds will be deposited in landfills nationwide. Chromium VI passes through membranes of cells “and is easily absorbed producing various toxic effects within the cells.” (Wood, 2003)

In the light of these serious future liability risks, corporations opt to “encourage” public schools to take on computers that they deem disposable. The rate at which computers become “ready for disposition” is increasing and yet the procedures for their storage and data

destruction cannot keep pace. In 2002 Michelle Galley of Education Week published an article on educators that were finally refusing donations of surplus equipment from computer donors. Galley reports how “Many schools find that they cannot use the older, outdated equipment that businesses and individuals want to give them, or that the cost of repairing and maintaining older technology is too high.” (Galley, 2002). Keith R. Krueger, the executive director of the Consortium for School Networking, highlights the problems related with receiving donated computers for public schools. Mr. Krueger says “The cost of free equipment is not free”. According to Kruger other factors affect the total cost of ownership such as the cost of replacement parts to maintain and upgrade the machines. The older machines require greater maintenance and often exert an additional salary burden on the schools. The older computers have a much shorter lifespan and thus the burden of eco friendly disposal is passed onto the public school. In certain cases, as highlighted by Galley's article, the public schools are recipients of software that may be too resource intensive to run on the older computers. In situations like these the donors are simply dumping their excess asset problem in the school district systems. The procedures in cases of PC dumping may often be fast track and potentially not follow adequate data destruction. According to Marlene Schick of the Central Indiana Educational Service Center, a branch of the state department of education, “Businesses have a financial incentive to donate machines, education technology experts point out, because they can receive a federal tax deduction for giving schools computers that are no more than 3 years old.” (Galley, 2003) Mr. Krueger concludes his statement with the comment that " We see too many schools that tell us horror stories about warehouses full of old, donated equipment they can't use, but politically they had to accept," ( Galley, 2003)

*Secure Data Destruction*

There are many methods of data destruction available in literature. In order to comprehend the methods of data destruction it is necessary to understand the concept of how data stores on computer hard disks. Data is stored on computers in Binary notation. In computer terminology, this two state condition is represented in binary notation by the use of 1s and 0s thus, two switches produce four codes - 00, 01, 10, 11 three switches produce eight codes - 000, 001, 010, 011, 100, 101, 110, 111 in mathematical terms:

Table 1

*Binary Data Represented in Switches/Alternatives*

1 binary digit provides 2 <sup>1</sup>	= 2 alternatives
2 binary digits provide 2 <sup>2</sup>	= 4 alternatives
3 binary digits provide 2 <sup>3</sup>	= 8 alternatives
8 binary digits provide 2 <sup>8</sup>	= 256 alternatives

[Courtesy Maguire, D.J., 1989. Computers in Geography, John Wiley and Sons, Inc., New York.]

The data translates to useful memory stores of data that are noted in units of ASCII code. By using binary notation, these codes can be converted into decimal numbers. This is done by counting from the right, the 8 bits are numbered 0 through 7, and signify as follows: Bit: 7 6 5 4 3 2 1 0 128s 64s 32s 16s 8s 4s 2s units (Maguire, 1989).

For example the combination 01010101 is no 128s, one 64, no 32s, one 16, no 8s, one 4, no 2s and one unit i.e.  $64+16+4+1 = 85$  in the ASCII code system, code number 85 is an upper case U thus to store a U, the system stores a byte with the bit pattern 01010101 (Maguire, D.J., 1989.) Memory then stores input for and output from the CPU as well as the

instructions that are followed by the CPU .The amount of memory stored is measured in bits, bytes, Kbytes (K, Kb, 103 bytes), Megabytes (Mb, 106 bytes), Gigabytes (Gb, 109), Terabytes (Tb, 1012). (Maguire, 1989). Computers have increased their storage capacity and complexity of software interpreters, however the binary storage remains generally the same. Hard disks are hard platters, made up of a substrate and a magnetic medium. The substrate can be aluminum alloy or a mixture of glass and ceramics. The platter's base material needs to be non-magnetic and capable of being machine tooled to a smooth finish. To facilitate data storage, both sides of each platter are coated with a magnetic thin-film medium. Interaction with the computer stores data in magnetic patterns, with each platter capable of storing a billion or so bits per square inch (bps) of platter surface. (pctechguide.com, 2003)

Data is recorded onto the magnetic surface of the disk As is the case in magnetic tape and floppy disks, the surface is treated as an array of dot positions, with each "domain" of magnetic polarization being set to a binary "1" or "0". The position of each array element is not identifiable in an "absolute" sense, and so a scheme of guidance marks helps the read/write head find positions on the disk. The need for these guidance markings explains why disks must be formatted before they can be used.

The simplest form of data destruction on a hard disk is a low level format. When a disk performs a low-level format, it is divided into tracks and sectors. “The tracks are concentric circles around the central spindle on either side of each platter.” Tracks are placed physically above each other on the platters and are clustered together into cylinders which are then further subdivided into sectors of 512 bytes each. A disk's smallest accessible unit is the sector (pctechguide.com, 2003).

Data is organized on a hard disk by the file system. File systems vary generally according to the operating system. The majority of PC file systems are compatible with Microsoft operating systems. This is because Microsoft operating systems dominate the desktop computer market. In most cases involving the disposal of surplus computers from University and Federal stores, the desktop computers predominately feature an operating system based on the Microsoft file system. The File Allocation Table, FAT, file system was first introduced in 1981. The purpose of FAT is to provide the mapping between clusters - the basic unit of logical storage on a disk at the operating system level - and the physical location of data in terms of cylinders, tracks and sectors - the form of addressing used by the drive's hardware controller. (pctechguide.com, 2003) The File allocation table contains an entry for all files stored on “the volume that contains the address of the file's starting cluster” (pctechguide.com, 2003) first cluster of the file.

The first version of FAT was called FAT12, could only work on a maximum partition size of 8MB. In 1984 by FAT16, was introduced, it increased the maximum partition size to 2GB. FAT16 is the most commonly available file system and it is compatible across a wide variety of operating systems, including Windows 95/98/Me, OS/2, and Linux.

NTFS is a newer and different file system from FAT that was introduced with first version of Windows NT in 1993. NTFS was designed to provide for greater privacy and security. NTFS supports access control and encryption of individual files and folders. The file system is more robust than FAT and less likely to suffer damage in the event of a system failure (Mikhailov, 2003).

When a file is deleted within the operating system what actually happens is that the operating system removes the reference to the file from the File Allocation Table. This reference contains the locator information with where on the disk the file was. The removal of the reference means the Operating System does not see this, it marks that area of the disk as free space. The data physically remains on the disk; only the reference pointing to it is removed. The data remains on the disk until another file is overwritten in that location. Even after a data overwrite it may be possible to recover data by studying the magnetic fields on the platter surface.

Data can easily be recovered by using free or commercial software. A secure precaution for proper disk drive sanitation is to wipe it before you "delete" it. There are many free and commercial programs applications that perform this task.

Secure data deletion is achieved by erasing magnetic media. It is necessary to overwrite it many times with alternating patterns in order to expose it to a magnetic field oscillating fast enough that it does the desired flipping of the magnetic domains in a reasonable amount of time. Certain applications are capable of high levels of data sanitation. SDelete (Secure Delete) is an example of one such application. SDelete securely deletes existing files, it implements the Department of Defense clearing and sanitizing standard DOD 5220.22-M. The Department of Defense in the clearing and sanitizing standard DoD 5220.22-M recommends the approach "Overwrite all addressable locations with a character, its complement, then a random character and verify" for deleting and sanitizing information on media disks (Standard DOD 5220.22-M, n.d).

Table 2

*US Department of Defense 5220.22-M Clearing and Sanitization Matrix*

Media	Clear	Sanitize
Magnetic Tape1		
Type I	a or b	a, b, or m
Type II	a or b	b or m
Type III	a or b	m
Magnetic Disk		
Bernoullis	a, b, or c	m
Floppies	a, b, or c	m
Non-Removable Rigid Disk	c	a, b, d , or m
Removabel Rigid Disk	a, b, or c	a, b, d , or m
Optical Disk		
Read Many, Write Many	c	m
Read Only		m, n
Write Once, Read Many (Worm)		m, n
Memory		
Dynamic Random Access memory (DRAM)	c or g	c, g, or m
Electronically Alterable PROM (EAPROM)	i	j or m
Electronically Erasable PROM (EEPROM)	i	h or m
Erasable Programmable (ROM (EPROM)	k	l, then c, or m
Flash EPROM (FEPR0M)	i	c then i, or m

Programmable ROM (PROM)	c	m
Magnetic Bubble Memory	c	a, b, c, or m
Magnetic Core Memory	c	a, b, e, or m
Magnetic Plated Wire	c	c and f, or m
Magnetic Resistive Memory	c	m
Nonvolatile RAM (NOVRAM)	c or g	c, g, or m
Read Only Memory ROM		m
Static Random Access Memory (SRAM)	c or g	c and f, g, or m
Equipment		
Cathode Ray Tube (CRT)	g	q
Printers		
Impact	g	p then g
Laser	g	o then g

[Courtesy US Department of Defense 5220.22-M Clearing and Sanitization Matrix]

#### Key

- a. Degauss with a Type I degausser
- b. Degauss with a Type II degausser.
- c. Overwrite all addressable locations with a single character.
- d. Overwrite all addressable locations with a character, its complement, then a random character and verify. This method is not approved for sanitizing media that contains top secret information.

- e. Overwrite all addressable locations with a character, its complement, then a random character.
- f. Each overwrite must reside in memory for a period longer than the classified data resided.
- g. Remove all power to include battery power.
- h. Overwrite all locations with a random pattern, all locations with binary zeros, all locations with binary ones.
- i. Perform a full chip erase as per manufacturer's data sheets.
- j. Perform i above, then c above, a total of three times.
- k. Perform an ultraviolet erase according to manufacturer's recommendation.
- l. Perform k above, but increase time by a factor of three.
- m. Destroy - Disintegrate, incinerate, pulverize, shred, or melt.
- n. Destruction required only if classified information is contained.
- o. Run five pages of unclassified text (font test acceptable).
- p. Ribbons must be destroyed. Platens must be cleaned.
- q. Inspect and/or test screen surface for evidence of burned-in information. If present, the cathode ray tube must be destroyed.

(DoD 5220.22-M Chapter 8, 2003 ).

## *Chapter 3*

### *Methodology*

This study focused on three research methods related to the awareness of issues concerning to data sanitization. The first is a survey of universities and the level of awareness as represented by their procedures posted for the disposal of surplus equipment. The intended population that the research targeted was the national university community. It was important for the study to examine educational institutions that have a considerable investment by the state and federal governments in the assets that are ultimately disposed. For this reason the total population is the institutions that are classified as the “Land Grant Institutions.” The congressional sponsor of the act establishing the land-grant university system was Justin Morrill. Morrill was primarily concerned for wider, “more democratic access to higher education to strengthen democracy” (Bonnen, 1998). Today the land grant university is often the flagship institution of a state and thus their compliance with protocol and procedures where critical issues are concerned is important.

The sample selection involved one land grant institution from each of the fifty states. This is intended to achieve a representative sample of sentiment and appreciated for proper disposal procedures.

The second investigation involved a localized sample of computers eligible for surplus at West Virginia University. The total population of this study was intended to cover all computers from the University departmental asset systems at a particular point in time. The nature of the disposal process is such that computers are continually flowing in and out of the storage facilities as they make their way from department desktops to the auctions/ donation

processes. The representative sample had to be of the typical state inventory in one of the computer storage facility at a particular point in time. For the purposes of ease of access and availability two storage facilities were chosen on the campus of West Virginia University. The two storage facilities were the pre-surplus store at the Health Sciences Center, which was chosen for its high potential for sensitive value data and the College of Business and Economics which was selected for its potential for relatively low value privacy data. The two samples represented opposite spectrums of the privacy risk scale and the testing would be on 100% of all desktop computers that were in storage at the facilities on a particular day during the academic year.

Finally the custodians of the facilities were interviewed for a possible comparison of the findings of the localized study against the perceptions of data security in the managers of the asset stores. The results of this study may offer the possibility of a generalization across departments at West Virginia University and with further study possible generalizations across other land grant institutions.

*Data Collection and Instrument Details.*

Data on the availability of published surplus procedures on Land Grant University websites was collected on a standard data collection form. The Process of collecting the data was done according to a specific set of guidelines. The information collected was reviewed to meet the following criteria.

1. The Land Grant University was reviewed for the presence of a website with administrative information relating to University operational procedures.
2. The University website was inspected for its postings of procedures for university departments to follow when retiring their computers
3. The posting, if present, was checked if it requires internal departments to delete data permanently from their own hard disks.
4. The instructions, if present on a land grants website were finally reviewed for instructions on how the departments should actually go about deleting the information from the hard drives.

Table 3

*Website Survey of State Flagship Universities*

Land Grant University	Are Surplus Procedures posted in the areas available for view by all departments, affiliates and extension services?	Are the postings available in a public internet or secured intranet?	Do the postings require internal donors to sanitize their hard drives before submitting the PC for surplus?	Do postings that require sanitation provide instructions on how to perform secure data deletion?
NAME	YES / NO	PUBLIC/ SECURED	YES NO NA	YES NO NA

The second instrument collected information about the data collected from the desktop computers and hard disks found at the pre-surplus storage facilities.

Table 4

*Data Collection of sampled computers in WVU inventory.*

Location of storage facility	Computer Type	Original Department	HD Identification	Size of HD	Amount of data	Sensitive Data present	Classification of data
------------------------------	---------------	---------------------	-------------------	------------	----------------	------------------------	------------------------

The last instrument covered questions presented to the management whose roles in the University system gave them custody over pre surplus assets. Interviews were conducted in an informal face to face setting. Responses were kept anonymous.

This document details the format of questions that were posed before custodians of surplus assets in the WVU system. The purpose of this instrument was to gauge the sense of awareness of the risks involved with data security and the steps being taken by these departments to ensure security.

Figure 1

*Interview Instrument Form*

Date

Role in WVU assets system

Questions

1. What does this department do with surplus assets?
2. What measures / procedures are performed on surplus computers prior to disposal?
3. Do you have any concerns over data security?
4. Have you considered any new procedures to ensure data security on assets sent to surplus?

*Data recovery and storage procedures*

For the purposes of data collection from the computers at the storage facilities, software applications were employed to inspect the data. The primary software application used was Easy Recovery Professional TM. This application facilitates the inspection of data on disks subjected to software or operating system deletion/formatting.

An additional application PC Inspector Easy Recovery, TM was used to restore deleted files from the hard disks. These applications are compatible with FAT, FAT32 and NTFS hard disks, which covered all of the hard disks found on the samples.

### *Statistical Treatment of Data*

Data from each of the hard disk inspections was recorded individually. Mean responses were calculated for those items that represent variable numerical data. Frequency distributions of each of the instrument results were computed with the use of SPSS software application.

The results of this study were used to contribute to discussion on

1. Gauging the level of awareness within the donor Universities for the need to prevent the loss of data to external recipients of surplus computers.
2. Assessing the level of risk in current pre surplus stores at Universities that could be addressed to avoid further liability.
3. Provide baseline data on the perceptions of surplus asset custodians and how these may be correlated with the potential for future breaches of private data.

## Chapter 4

### *Results*

The results of the research were intended to provide answers to the original research questions which were:

1. Are the recipients of surplus computers currently also the recipients of sensitive and inappropriate data?
2. What are the risks of the information to educational recipients such as K-12 schools and what steps should be taken?
3. Has the complexity of proper disposal procedures resulted in sensitive data being handed down to public schools and other programs?

Some departments and colleges have posted specific programs for the proper destruction of surplus data. These methods of data destruction vary in complexity. The levels of complexity in carrying out data disposal may be a factor in some data breaches. It may be significant for the study of these procedures to be analyzed for the impact that training and understanding on the part of the custodians may have in instances of information breaches. There are different methods of effectively deleting data permanently, however many of these involve using software that addresses the data clusters on the hard disks. These applications may be difficult to understand for the typical inventory clerk, who in most cases is the last person to oversee the disposal of assets destined for the educational platforms. The study aims to review the different types of posted instructions on the websites of Universities that document surplus procedures and examine the level of detail in the documented procedures. This level of detail may provide insight on how the procedures may need to be supplemented

by training programs or any remedies that may address this issue and prevent more data breaches to the public communities.

The data analysis of the Surplus procedures of Land Grant institutions yielded the following results.

1. The land grant university was reviewed for the presence of a website with administrative information relating to University operational procedures.
  - a. The Data on whether or not the institution had a posting relating to surplus procedures on its website is reflected in Table 5.

Table 5

*Presence of a website with administrative surplus information*

	Count	Percentage
NO	17	34
Yes	33	66
Total	50	100

Sixty six percent of all Land Grant institutions had a posting on their main web interface that directed internal departments and affiliates on how to deal with surplus assets.

2. Are the postings available in a public internet or secured intranet?

Postings were whether in publicly accessible areas or in intranets which exclude members of extension services and University affiliates.

The distribution of these across institutions is reflected in the Table 6.

Table 6

*The distribution of intranet vs. internet based instructions*

	Count	Percentage
NA	17	34
Public	29	58
Secured	4	8
Total	50	100

The Institutions Classified as NA had no procedures posted at all. The data reflected that 58 % of all Land Grant Institutions have data in an accessible public portal.

8 % of all LGI's posted procedures in intranets or closed portions of their websites.

3. The postings, if present, were checked if they required internal departments to delete data permanently from their own hard disks.

This action of inspecting the posting for a requirement in the actual posting for University faculty and staff to sanitize hard disks before submission yielded the following results displayed in Table 7.

Table 7

*Flagship institutions that advocate data sanitation*

	Count	Percentage
NA	23	46.0
No	16	32.0
Yes	11	22.0
Total	50	100.0

Only 41% of schools that had public postings specified the need for sanitation.

4. The instructions, if present on a land grant website were finally reviewed for instructions on how the departments should actually go about deleting the information from the hard drives. This is intended to resolve the question of if “the complexity of proper disposal procedures resulted in sensitive data being handed down to public schools and other programs?”

The criterion in this test inspected posted procedures for specific procedures on how to sanitize data. The information would be read by the departmental custodian at the pre-surplus stage. The test returned a distribution of results listed in Table 8.

Table 8

*Institutions that provide data sanitation instruction procedures*

	Count	Percent
NA	14	28.0
NO	27	54.0
YES	9	18.0
Total	50	100.0

Results show that 18% of all land grant universities post procedures with instructions on how to sanitize data drives before sending equipment to surplus

The research question “Are the recipients of surplus computers currently also the recipients of sensitive and inappropriate data?” is answered in the second instrument.

Data from the localized test provided information on the status of the data security at the West Virginia University Health Sciences Center pre surplus storage and the Surplus storage at the West Virginia University College of Business. The two storages facilities had computers distributed according to the types shown in Table 9.

Table 9

*Distribution of computers Sampled*

Computer Type	Number of Computers	% Percentage of Computers
API 386	1	2.1
Compaq Presario	1	2.1
Dell Dimension	12	25.0
Dell Optiplex	10	20.8
Dell Optiplex PC	1	2.1
E-Machines 330	1	2.1
Gateway G6300	2	4.2
Gateway-2000 PC	5	10.4
Gateway E311	1	2.1
Gateway PS120 PC	1	2.1
Gateway 2000 PC	6	12.5
Gateway 2000/P5	1	2.1
Gateway E311	1	2.1
Gateway LP	1	2.1
Gateway PS-66	1	2.1
Gateway PS120 PC	2	4.2
Gateway WPS166	1	2.1
Total	48	100

Table 10

*The age distribution of the computers sampled*

Date of Manufacture	Count	Percent
1995	5	10.4
1996	9	18.8
1997	7	14.6
1998	26	54.2
1999	1	2.1
Total	48	100

It was possible to determine the original departmental use of the desktop computers inspected in some cases. The results of the sources are displayed in Table 11.

Table 11

*Original Source of Computers Sampled*

Original Source of Computers	Count	Percent
B&E Computer lab	11	22.9
FINANCIAL AID	1	2.1
HSC MAINTENANCE	3	6.3
HSC NURSING	1	2.1
STUDENT HEALTH	2	4.2
Undetermined	30	62.5
Total	48	100

As shown above it was not possible to determine the original use of 62.5 % of the computers inspected. This was due to cannibalization of computer components such as the hard disks, cases and other identifying components. In the identifiable cases information on their original owners was available through the information on the hard drives and information provided by the custodians of the storage facilities.

Data recovered was measured in megabytes. The computers that still had hard disks were inspected for the nature and quantity of data. The findings are displayed in the Table 12.

Table 12

*The amounts of data recovered on stored hard disks*

Data in Megabytes	Number of computers	Percentage of Total Sample
1000	1	2.1
103	1	2.1
200	2	4.2
451	1	2.1
5	1	2.1
540	1	2.1
70	2	4.2
75	1	2.1
80	1	2.1
90	1	2.1
Malfunctioning	1	2.1
Removed	14	29.2
Sanitized	21	43.8
Total	48	100.

Table 13

*Types of data recovered from sampled computers*

	Count	Percentage
No Data Recovered	35	72.9
Operating System and General data	12	25
Private and Sensitive data	1	2.1

The results reflected that the spontaneous inspections of the two stores yielded 2% (1 computer in the sample of 48) that contained sensitive data.

Table 14

*The distribution of data by sensitivity of information recovered.*

NO	47	97.9
YES	1	2.1
Total	48	100

## Chapter 5

### *Discussion*

The survey of Land Grant Institutions (LGI's) showed high numbers related with their level of awareness on issues related to data sanitation. The time and effort taken into posting procedures onto bulletins for use by faculty and staff is a reflection of the degree of gravity the institution places on data security. In the inspection study it was significant to note that 34 % of the state flagship universities do not address the issue of surplus computers and their hard disks at all. This can be interpreted to mean that in these institutions faculty and staff often has to use their own initiative to determine the correct measures for discarding computers and donating them to other environments. These 34% also do not have any assistance directly posted to help them find out how they can secure the data they may have on the hard disks. This is particularly important in a local sense to the institution. In some cases the University may not place postings because the responsibility of data sanitation is placed in the hands of the surplus store custodians. This exposes great amounts of University data from departments like the medical school and human resources at the mercy of surplus clerks who may not be suited for the information they become exposed to.

The data also reflected that 8% of the flagship universities opted to place their procedures relating to surplus equipment in secured intranets. This scenario works fairly well for localized faculty and staff. The problem presents itself in cases where the university has assets in extension units and rural satellites. When assets are sent to central stores from these locations, without adequate guidance data may remain present. Intranets offer access to operational procedures to computers and users who are within the local purview of the University.

Twenty nine universities out of the fifty land grant institutions did take the step of publishing surplus procedures on the internet for all users. This is the majority of the flagship institutions. The fact that so many of the institutions have opted to post these procedures in this accessible format reflects their appreciation of the risks that negligence of data security represents. The problem is that only 41% of schools that had public postings specified the need for sanitation. This reduces the schools that tackle the problem of data sanitations directly to 11 from the sample of 50 flagship Universities. The sample of schools that then show faculty and staff how to actually sanitize information is smaller yet. In the data sets only 9 Schools, 18% of the Land grant universities, post procedures that advice faculty and staff on how to sanitize disks before sending them to the surplus stores. The statistics are clear enough to support a conclusion on the levels of awareness reflected by universities. The next instrument involved two spontaneous tests of surplus stores at WVU. The data retrieved from the tests gave a localized sample of the likelihood of data being found at a land grant institution that does not post its instructions for surplus procedures online. The first Instrument determined that West Virginia University was one of those land grant institutions that did not post its requirements for use by all internal faculty and staff before assets are sent to surplus.

In this test, 48 computers were inspected from the two locations. All the computers in both samples were less than nine years old however, 54 % of the computers were manufactured in 1998. In terms of asset donation , computers from the period 1997- present are generally considered still useful and are often passed on to educational environments where possible. During the procedures of the research inspections it was noted that 11 computers, 22 % in the sample had been earmarked for a program that sent the surplus computers overseas to the

African nation of Mali. The computers that had hard disks could be identified to their original department of purchase. In the sample tests, using information from custodians and hard disk 37.5 % of the sample could be identified for its original donors.

Computers that were found with data ranged in the amount of data recovered. The highest amount of data on a single drive was 1 gigabyte of unsecured data and the lowest was 5 megabytes. Thirteen computers were found with functioning retrievable data on their hard disks, this represented 27 % of the total sample.

The sample yielded non sensitive data that related to general operations such as maintenance engineering and a fax server with no documents on 25% of the units. One unit did have highly sensitive data from the office of financial aid. The sensitive data find reflected 2% of the total sample size but the liability that the data itself potentially exposed is significant.

Data from the third instrument, the interviews with custodians, was unavailable at the time of data submission and publication. The Custodians were contacted for an effort to obtain responses on the issues resulting from the tests but efforts by the investigator were unfruitful.

### *Conclusions*

The levels of awareness within the fifty land grant institutions investigated in the study were significantly low. Institutions are not adequately addressing the risks associated with improper disposal of surplus computers. If only 33 of the fifty schools consider the issue worth of any web space, this is indicative of a potential problem. The institutions are often leaders in education for their home states and they set the pace of development for the smaller colleges and universities. If the flagship institutions do not take the issue of data security of assets to the secondary market seriously, then it stands to reason that the satellite schools and affiliates are in similar circumstances.

The numbers of schools that take the issue as far as requiring sanitation is low too but it may be a trend that could increase over the next few years. Data sanitization is a complex process so simply requiring faculty and staff to “sanitize” their hard disks may result in many computers being found with data simply placed in the “recycle bin” .

None of the land grant institutions offered training for faculty and staff on how to personally be accountable and sanitize their own disks. Free tools are available that could be proliferated via the web making the process of data security more complete.

The tests also reflected that the process of donating computers to the educational market is still on going. The school in Mali could have been the recipient of a computer with the financial and tax records of students who may have applied for financial aid at WVU within the last nine years. The level of caution when dealing with assets to the secondary market needs to be greatly elevated.

The localized sampling may help in assessing the level of risk that the universities expose themselves to when the pre surplus stores are not inspected for compliance to University surplus procedures. The donors need to evaluate the process of sending surplus assets to school districts. The examples detailed in the report show how the trend appears to point toward the public schools being used as “dumping grounds” for assets that may not be as useful to the students they teach.

The numbers of newspaper and TV reports provide many anecdotal instances of data loss and breach; however the lack of academic reading on the matter is indicative of the low level of awareness on this topic. The introduction of penalty related legislation like HIPAA is only a year old. This means that the actual impact of data breaches may not yet affect the bottom lines of donors, both tertiary and corporate. The impact of older legislation like EO 12999 is that there may already be thousands of potential breaches in the educational market that will only surface when the school districts themselves decide to hold auctions of the assets they received but never used.

### *Recommendations*

Data security and sanitization is not an exact science. The magnetic nature of hard disk technology makes the absolute destruction of data while keeping the disk intact currently impossible. The most practical solution may be to keep the computer disks within the operational system of the donors departments and agencies. The recipients of surplus computers may have to add an additional cost of hard disks and turn to free open source operating systems like Linux. Further research into the advancements in sanitization methods and technology may provide easier practical methods of safeguarding data in the future.

The correlation of results from the localized tests would be further enhanced with a nationwide study of stores around the fifty land grant institutions in the United States. The data in gigabytes that is already available in storage facilities around the nation may be of interest to researchers who wish to pursue this study in greater detail.

Subsequent to the localized test at West Virginia University Health Sciences Center, a mandate was given to send all desktop computers, (with drives intact) to a landfill in West Virginia. A study on the impact of this directive on the environment and community and its effectiveness on addressing the security issue may also be research worthy.

## References

- Hudson T. (2001, October 10). Wrong turn gets schools computers. Tri-City Herald.com. Retrieved November 16, 2003, from <http://www.tri-cityherald.com/news/2001/0810/story5.html>. Accessed November 2003.
- Micek, J.L. (2001, April 5) Sensitive data found on discarded Government PCs. *The NewsFactor Network*. Retrieved October 30, 2003, from <http://sci.newsfactor.com/perl/printer/8727>
- Brain, M. (2003). How hard disks work. HowStuffWorks.com . Retrieved November 17, 2003, from <http://computer.howstuffworks.com/hard-disk1.htm>
- Wolfe, C. (2003, February). Discarded computer had confidential medical information. *Associated Press*. Retrieved November 18, 2003, from [http://www.onlinesecurity.com/Community\\_Forum/Community\\_Forum\\_detail106.php](http://www.onlinesecurity.com/Community_Forum/Community_Forum_detail106.php)
- Health Insurance Portability And Accountability Act. (1996). Public Law 104-191 104<sup>th</sup> Congress. Retrieved November 17, 2003, from <http://hippo.findlaw.com/title2.html#Anchor59182>
- Physical safeguards to guard data integrity, confidentiality, and availability. (2003). *Center for Medicare & Medicaid Services*. Retrieved November 17, 2003 from <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/sec07.asp>
- Techweb Encyclopedia (2003). Hard drive. Retrieved November 10, 2003 from

<http://www.techweb.com/encyclopedia/defineterm?term=hard+drive&x=19&y=10>

Public Law 104-191. Behavenet.com. Retrieved November 17,2003 from

<http://www.behavenet.com/capsules/law/HIPAA.htm>

Techweb Encyclopedia (2003). Desktop Computer. Retrieved November 10, 2003, from

<http://www.techweb.com/encyclopedia/defineterm?term=desktop+computer&x=12&y=12>

Techweb Encyclopedia (2003). CPU. Retrieved November 10, 2003, from

<http://www.techweb.com/encyclopedia/defineterm?term=cpu&x=29&y=12>

Starks, D. (Producer). (2003, February 10). *6News*. [Television broadcast]. Charlotte: National Broadcasting Corporation.

Office of Property Disposal. (2003). Federal Property And Administrative Services Act Of 1949 As Amended. Retrieved November 23, 2003, from

[http://rc.gsa.gov/ResourceCenter/laws\\_regs\\_all/Fpasa49/49Act.htm](http://rc.gsa.gov/ResourceCenter/laws_regs_all/Fpasa49/49Act.htm).

The Stevenson-Wydler Technology Innovation Agreement of 1980, PL 96-480. (1980).

The National Institute of Mental Health. Retrieved October 31, 2003 from

<http://intramural.nimh.nih.gov/techtran/legislation.htm>

Office of the Press Secretary. (1996, April 17). Executive Order 12999: Educational Technology. Washington D.C: The White House.

Vail, K. (2003, September). School technology grows up: Good-bye to the gee-whiz - - the new generation of ed tech is all about solutions. *American School Board Journal*, 190(9), 34-37.

Johnson, K.A. (2000, June 14). Do computers in the classroom boost academic

- Achievement. Report of the heritage center for data analysis. Washington, DC : The Heritage Foundation.
- U.S. Department of Education. (1995). Technology's role in education reform: Findings from a national study of innovating schools. Office of Educational Research and Improvement. Retrieved November 19, 2003, from <http://www.ed.gov/PDFDocs/techrole.pdf>
- Salpeter, J. (1998). Taking stock: What's the research saying? *Technology And Learning*, 18 (9) ,24-30.
- Kimble, C. (1999). The impact of technology on learning: making sense of the research. *Mid-Continent Regional Educational Laboratory*. (pp1-6).
- Healy, J.M. (1998). *Failure to connect*. New York: Simon & Schuster.
- Glennan, T.K.Jr., Baer, W.S. Prunell, S., Farnsworth, G., & Schuyler, G. (1997). *Surplus federal computers for schools an assessment of the early implementation of E.O. 12999*. Critical Technologies Institute Rand Publishing.
- Haddock, B. (January, 2000). SRS computer security probed. *Augusta Chronicle*. Retrieved November 19, 2003, from [http://augustachronicle.com/stories/011500/tec\\_066-6788.000.shtml](http://augustachronicle.com/stories/011500/tec_066-6788.000.shtml)
- Hensel, K. (Producer). (2002, May). Congressman buyer demands answers about security breach. *A News 8 I-team Investigative Report*. [Television broadcast]. Indianapolis: WorldNow and Wish-TV.
- Dixon, C. & Whitfield, F. (Presenters). (2002, March 1). CNN Live Today : Computers Sold To Public Filled With Secret Information. [Television broadcast]. Transcript# 030123CN.V75. Cable News Network

Hart, P.(2003). Outdated computers? Pitt details right way to dispose of equipment.

*University Times*. University of Pittsburgh, 35, 22.

Senate Bill 807, (March, 2001). An Act Concerning Computer And Electronic Solid Waste Management For The State Of Arkansas; And other Purposes : An Act Concerning Computer And Electronic Solid Waste Management. 83<sup>rd</sup> General Assembly, state of Arkansas.

University of Nebraska-Lincoln. (2003). Surplus Equipment. Retrieved November 17, 2003 from <http://www.cba.unl/its/policy/surplus.html>

Frank, D. Jr. (2002). Where should that old computer go? *Caribbean Business*, 30, p36.

Disposition Of SMCC Surplus Equipment. Faculty Handbook. Retrieved

November 19, 2002, from

<http://www.smcc.edu/facultyhandbook/FacultyHandbookp42.htm>

Wade, B. (2001). Life after death for the nations pcs. *Amererican City & County*. March 2001 Edition, pp22-26.

Wood, L. (2003, November). Old PCs toxic in landfill sites. *The Gault Review*. Retrieved

November 19, 2003, from [http://www.galtglobalreview.com/business/toxic\\_pcs.html](http://www.galtglobalreview.com/business/toxic_pcs.html)

Quain, J.R. (2001). Upgrade create digital landfill. *Popular Science*, 258(2), p37.

Dangerous disclosure: Action update from VA Medical Center. (2002, May 16). News 8

I-Team Investigating Report. [Television broadcast]. Indianapolis: WorldNow and Wish-TV.

Eastwood, A. (2002, October 14). Garbage day: Tech trash threatens to put our economy

in the dumpster. EBSCOhost. Retrieved November 19, 2003, from

[http://web14.epnet.com/citation.asp?tb=1&\\_ug=db+0%2C3%2C6%2C7+In+en%2](http://web14.epnet.com/citation.asp?tb=1&_ug=db+0%2C3%2C6%2C7+In+en%2)

Dus+...

Galley, M. (2002, June). Schools no longer to accept used computers. *Education Week*, 21, p8.

Maguire, D.J. (1989). *Computers in geography*. Essex: Longman. Chapter 7 & 10.

Pctechguide.com (2003). Storage/Hard disks. Retrieved November 19, 2003, from

<http://www.pctechguide.com/04disks.htm>

Mikhailov, D. (n.d). NTFS file system. Retrieved November 19, 2003, from

<http://www.digit-life.com/articles/ntfs/>

Standard DOD 5220.22-M/ NISPOM 8-306. (n.d). Retrieved November 20, 2003 from

<http://www.zdelete.com/dod.htm>

Bonnen, T. (1998). The land grant idea and the evolving outreach university. In

Lerner, R.M. & Simon, L.A.K. (EDs), *University-Community Collaborations for the twenty-first century: outreach to scholarship for youth and families* (pp.25-69). New York, NY: Garland Publishing.

## Appendices

### Appendix A

University	Surplus Procedures Posted	Posting Public or Secured	Posting Requires Data Sanitation	Posting Instructions Data Sanitation
Auburn University	YES	Secured	NA	NA
Clemson University	YES	Public	YES	NO
COLORADO STATE UNIVERSITY	YES	Public	YES	YES
Cornell	YES	Public	NO	NO
Iowa State University	YES	Public	YES	NO
Kansas State University	NO	NA	NO	NO
Louisiana State University	NO	NA	NO	NO
Michigan State University	NO	NA	YES	NO
Mississippi State University	NO	NA	NO	NO
Montana State University	NO	NA	NO	NO
New Mexico State University	NO	NA	NO	NO
North Carolina State University	NO	NA	NO	NO
North Dakota State	NO	NA	NO	NO
Ohio State University	NO	NA	NO	NO
Oklahoma State University	YES	Public	NO	NO
Oregon State University	YES	Public	NA	NA
Pennsylvania State	YES	Secured	NA	NA
Purdue University	NO	NA	NA	NA
Rutgers University	YES	Public	YES	YES
South Dakota State	YES	Public	NO	NO
Texas A&M University	YES	Secured	NA	NA

University of Alaska Fairbanks	NO	NA	NA	NA
University OF Arizona	YES	Public	YES	YES
University OF Arkansas	NO	NA	NA	NA
University OF California, Davis	YES	Public	NO	NO
University of Connecticut	YES	Public	YES	YES
University of Delaware	NO	NA	NA	NA
University of Florida	YES	Public	NO	NO
University of Georgia	NO	NA	NA	NA
University of Hawaii, Manoa	YES	Public	NA	NA
University of Idaho	YES	Secured	NA	NA
University of Illinois, Urbana- Champaign	YES	Public	NO	NO
University of Kentucky	YES	Public	YES	YES
University of Maine, Orono	YES	Public	NO	NO
University of Maryland	YES	Public	NO	NO
University of Massachusetts	YES	Public	NO	NO
University of Minnesota	YES	Public	NO	NO
University of Missouri	YES	Public	NO	NO
University of Nebraska, Lincoln	YES	Public	NO	NO
University of Nevada, Reno	YES	Public	NO	NO
University of New Hampshire	YES	Public	NO	NO
University of Rhode Island	NO	NA	NA	NA
University of Tennessee, Knoxville	NO	NA	NA	NA
University of Vermont	YES	Public	YES	YES
University of Wisconsin-Madison	YES	Public	NO	NO
University of Wyoming	YES	Public	YES	YES
Utah State University	YES	Public	NO	NO

Virginia Tech	YES	Public	YES	YES
Washington State	YES	Public	YES	<b>YES</b>
West Virginia University	NO	NA	NA	NA

## Curriculum Vitae

Ngoni Murandu

[nmurandu@hsc.wvu.edu](mailto:nmurandu@hsc.wvu.edu)

---

441 Broadway Ave

Morgantown West Virginia 26505

Work 304-293-1148

Home 304-598-8559

### Education

1990 St. Johns High School

1992 St. George's College

Majors Accounting, English Literature & History

Awarded "A" level achievement Prize for Grades earned in the University Cambridge  
Syndicated Examinations.

**BA Degree West Virginia University Management of Information Systems**

**Currently in Final Semester of a Masters in Technology Education at WVU**

*Professional Experience*

**2000- Current      Director of Information Technology, West Virginia University  
Health Sciences Center, School of Dentistry**

Directed operation of the information systems division. Instrumental in the implementation of the *first US* application of AXIUM, dental management system. Introduced digital imaging and enhanced presentation methods to faculty body. Trained faculty, students and staff on information technology. Major roles in financial reporting, report writing and audit of internal controls. Participated in various research projects that were published on a national level. Participated in ADEA forums for dental education.

Introduced new types and application of technology including an intranet, online publications and Oracle and SQL Databases. Development of budget controlled inventory replenishment cycles. Installed the only AXIUM based instrument tracking application in the United States and downloading of data from database extractions onto PDA's.

**1998-1999      SYSTEMS MANAGER Centers for Disease Control, NIOSH Division.  
Records Management, (HGO Technologies)**

Managed the archiving and distribution of CDC documents, classified and non-classified, used in the HHE application PUNDIT. Maintained an NT, NetWare and desktop network.. Participated in many projects including intranet development, searchable databases and cross-platform Information distribution.

### **1998 Desktop/Network Tech WVU School of Business and Economics**

Maintained 300-user network of desktop computers. Assisted in implementation of large volume software projects, upgrades and installation. Controlled inventory processes and help desk for standard troubleshooting.

### **1997 IBM Process Specialist**

Specialist Computer systems designer catering for accounting systems. Involved the installation and support of software for large companies. Presentation to senior members of Management of system demonstrations and setup. Consulting on the optimum use of information technology. Advanced exposure to the latest and most useful packages in software. Exposure to a number of contacts within the software world and experience in initial contracts. Experienced in different company systems and developed an ability to adapt to fit client requirements. Special Projects such as, Planned, designed and implemented the re engineering of the Accounts for National Oil Company.

### **1996 Leopard Rock Hotel, Golf Course and Casino FINANCIAL MANAGER**

Manager over the all sections of accounting control. Preparation Through to Final Presentation of 4 Companies Accounts, Management reports. Daily payment s management. Food and beverage cost management.

### **1995 Victoria Falls Safari Lodge Front Office & Systems Supervisor**

From the pre opening stages of the project Installed and trained the entire Front office System. Supervised all system procedures including negotiations with software and hardware

suppliers, managed reservations, Guest Ledgers & Front office. Coordinated Data Collected & input Assisted in Timeshare operations and sales. Invited to Become Three Cities First Zimbabwean Management trainee.

**1993 - 1994 Price Waterhouse Chartered Accountants Audit Junior (Served 14mths articles of clerkship)**

Dealt with AUDITING; Cashbook & bank, interest calculations, fixed assets, share capital adjustments, debtors, profit & loss accounts, creditors and stocks

**1994 - 1994 Leopard Rock Hotel, Golf Course and Country club**

***Internal Auditor***

Daily Funds Analysis Report & Management. Redesigned Hotel Laundry Setup fixed asset register (program on Lotus), Set up House accounts monitoring program. Highly involved in setup of Casino Float Recon Program. Revamped accounts stationery Layouts. Redesigned Switchboard Funds recording Procedures. Worked on reconciling prior months Cashbook. Prepared and Executed Hotel Uniform and Linen budgets.

**Computer Systems Experience**

AXIUM, Oracle , Access, Crystal Reports and Crystal Enterprise. Advanced work with Spreadsheets and all Office suites. Systems administrator abilities with windows 98-ME NT and 2000-XP. Considerable experience with Netware and Knowledge of UNIX, Aix and OS/2 operating systems. Advanced capabilities with Internet technology, HTML, ftp and mail & server daemons. Expert in Peachtree, SAP and Oracle accounting applications.

Exposure includes J.B.A software, Lanmark, Proteus Accounting. Digital imaging , Image servers , video streaming and PDA interfaces.

All forms of hardware maintenance.

***Objective***

UP UP UP. Motivated by project completion and achievement.

**Awards & extracurricular activities**

1986 Prefect at North Park School, leading Drama actor, I St. Chess Team

1989 Vice Chess Captain St. Johns High School.

1990 Chess Captain St. John's High School

1991 Awarded Best Chess Player at St. John's High School

1992 Chess Captain St. George's College, Johanny House Prefect

Colors Chess Interact Society Debating Society, and IV XV Rugby. Represented St.

George's at Inter schools Business Management Games

1993 Outward bound endurance training course

**Languages**

English & Shona,

***Community activities***

Athol Evan's Service Project

WVU Community Based Management Project.

## **REFERENCES**

Shelia Price

West Virginia University Asst Dean

Phone Number: 304-293-1980

Email Address: sprice@hsc.wvu.edu

Reference Type: Professional

Lok Nguyen HGO

Technologies Manager

Phone Number: 304-598-2539

Email Address: jomalley@hgo.net

Reference Type: Professional

Carol Henry

West Virginia University Director of Information Systems

Phone Number: 304-293-7934

Email Address: cheny2@wvu.edu

Reference Type: Professional

Priscah Simoyi

West Virginia University Instructor

Phone Number: 304-293-1291

Reference Type: Personal

Clark St Clair

West Virginia University Student Advisor

Phone Number: 304-293-8292

Email Address: [clark.stclair@mail.wvu.edu](mailto:clark.stclair@mail.wvu.edu)

Reference Type: Professional