MEMORANDUM

TO: Members, Utah State Board of Education

FROM: Martell Menlove, Ph.D.
Chief Executive Officer

DATE: April 4, 2014

INFORMATION: Current Practices for Information Technology (IT) and Data and Statistics Sections

---

Background:
Concerns about data security and data gathering practices are voiced regularly. This includes USOE policies and procedures as data is collected, stored, and reported to state and federal agencies.

Key Points:
Staff from IT and Data and Statistics will present information on current data policies and procedures which will include data security policies and procedures, FERPA, and other current practices. This will include a description of the data that is collected, how it is collected, the security protocols in place, etc. Staff will respond to questions from Board members.

Anticipated Action:
The Board will receive the information provided and may request additional information.

Contact: Judy Park, Associate Superintendent, 801-538-7550
Jerry Winkler, Director, Information Technology, 801-538-7842
Aaron Brough, Coordinator, Data and Statistics, 801-538-7922

250 East 500 South P.O. Box 144200 Salt Lake City, UT 84114-4200 Martell Menlove, Ph.D., State Superintendent of Public Instruction

Utah STATE OFFICE of Education

USOE State Longitudinal Data System

GENERAL INFORMATION

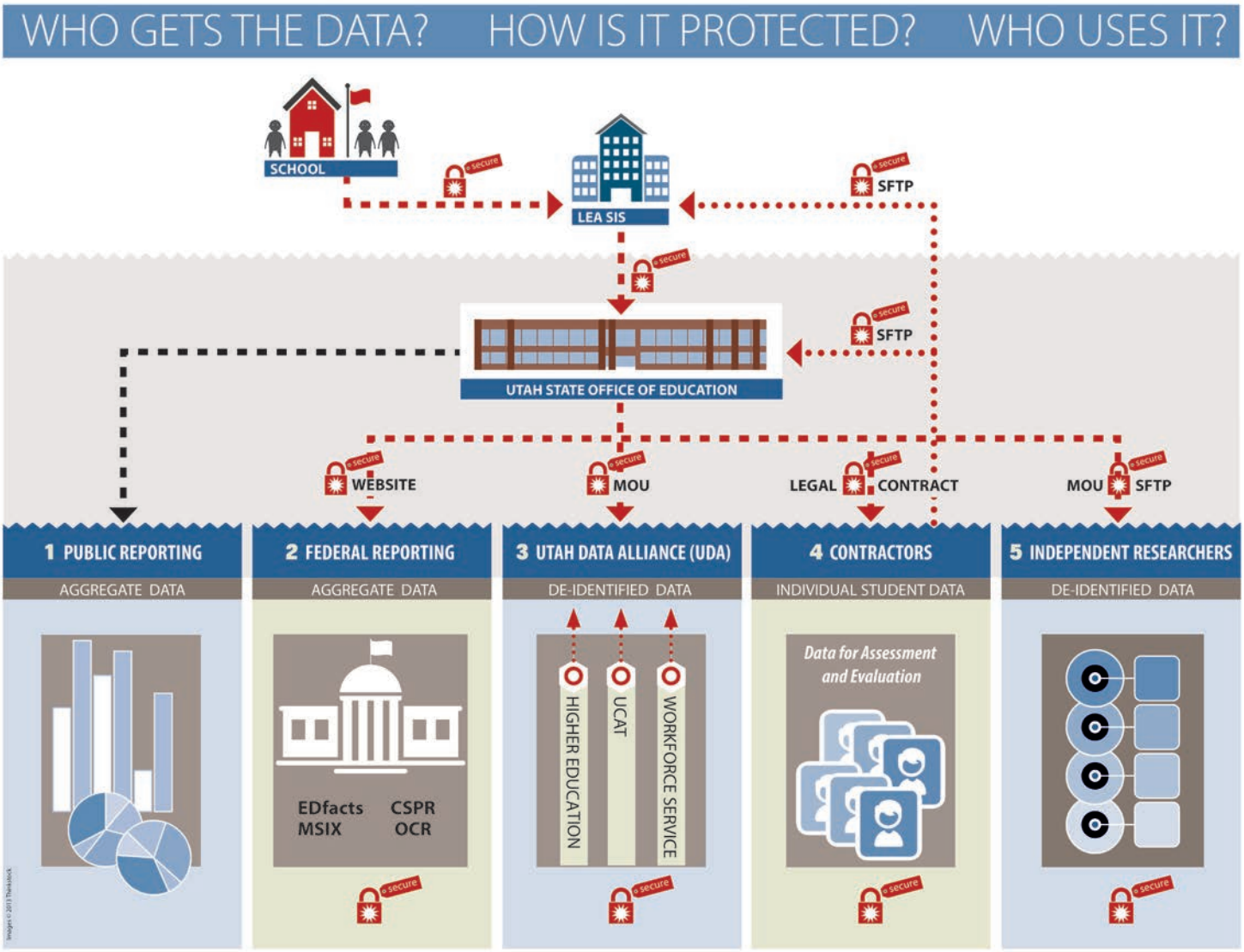
- The Statewide Longitudinal Data System allows Utah to continue efforts to provide schools and districts with necessary data to inform instruction and ensure every student receives the most appropriate education possible.
- The Utah State Office of Education (USOE) has had a student level data warehouse since 1998.
- The USOE has reported aggregate data to the federal government since the 1970s.
- **The Common Core Standards do not contain requirements related to data collection or data reporting. The Common Core Standards have no impact on data collection or reporting.**
- **The new computer adaptive assessment system (SAGE) will not change any of the data that are collected or reported.**
- The USOE collects a variety of information on Utah students, including such things as name, date of birth, race/ethnicity, gender, special education, performance on state assessments, status related to English language proficiency, students who qualify for free/reduced priced meals, grades, credits, enrollment dates, school and district.
- The USOE **DOES NOT** collect information on political affiliations or beliefs; sexual behavior or attitudes; religious practices, psychological or behavior testing, DNA, student address or e-mail, or income of the student or family.
- Required data reports are only provided in the aggregate, meaning only state, district, school and grade level data are provided. **Not student level data**. Note: For the Migrant Student Program (MSIX), when parental consent is given on the certificate of eligibility, student level data is submitted to the federal government.
- USOE uses industry standards for the collection, transfer, storage and reporting of data. All data are stored in secure, encrypted databases. USOE's Data Governance Plan includes policies and procedures that meet industry standard requirements for the security and protection of student level data. The USOE Data Governance Board reviews all research requests and approves only those requests that are appropriate and meet the requirements set by the Board of Education (R277–487).
- USOE received a federal grant in 2007 to develop a Utah Transcript Record Exchange (UTREx) that improved the secure electronic transport of data from the schools/districts to USOE and created a mechanism for electronic data to be transferred when a student moves from one district to the next. This was not "Race to the Top" money and has no connection to the Common Core.
- USOE received a federal grant in 2010 to develop the Utah Data Alliance (UDA). The UDA is a multi-agency partnership that facilitates the reporting of longitudinal data from the Utah State Office of Education, Utah System of Higher Education, Utah College of Applied Technology and the Utah Department of Workforce Services. This data partnership facilitates the reporting of data such as the Governor's goal of 66% of Utah residents to hold a postsecondary degree or certificate by the year 2020. The federal grant was ARRA (American Recovery and Reinvestment Act) money. This was not "Race to the Top" money and has no connection to the Common Core.

Detailed information about the data collected and reported at USOE is available on the USOE website

http://www.schools.utah.gov/computerservices/Services/Data-Clearinghouse/Data_Clearinghouse_Update_Transactions_20130123.aspx

http://www.schools.utah.gov/warehouse/Specifications/Warehouse-Data-Dictionary.aspx

http://www2.ed.gov/about/inits/ed/edfacts/index.html



TERM	DEFINITION
AGGREGATE	Elements of data combined to represent a group that is greater than 10 students
ASSESSMENT	State mandated assessments such as Criterion-Referenced Tests (CRTs)
LEGAL CONTRACT	This must be signed before any data can be shared with a contractor
CONTRACTOR	A company or person with a formal contract with USOE to do a specific job
CSPR	Consolidated State Performance Report
DE-IDENTIFIED	Data that has been adjusted to prevent the identification of a student
EDFACTS	U. S. Department of Education data collection system for data required by federal law
INDEPENDENT RESEARCHERS	Researchers associated with a university or private company requesting data for purposes of conducting research
LEA	Local Education Agency
MOU	Memorandum of Understanding
MSIX	Migrant Student Information Exchange —includes some student level data
OCR	Office for Civil Rights
SFTP	Secure File Transfer Protocol; the secure, encrypted transfer of data files
SIS	Student Information System; the technology that each LEA/school uses to collect student data
UCAT	Utah College of Applied Technology
UTAH DATA ALLIANCE (UDA)	A multi-agency partnership that facilitates the reporting of longitudinal data from the USOE, Utah System of Higher Education, UCAT and the DWS
UTAH STATE OFFICE OF EDUCATION	The State Office of Education (USOE) is responsible for the collection, storage and report ing of data
UTREX	Utah Record Exchange; the technology for LEAs to securely transfer data to USOE
WORKFORCE SERVICE	Department of Workforce Services (DWS)

Data Governance and Management

Updated November, 2012

Contents

Overview

Accurate, relevant and timely data can inform policy makers and educators in setting goals, targeting interventions, identifying strengths, making policy, and monitoring progress. Accurate, relevant and timely data requires that the appropriate people have access to the data they need when they need it and know how to effectively and accurately report the data. This must also be balanced by privacy concerns and proper data use.

The Utah State Office of Education (USOE) has developed a data governance structure based on proven data governance practices and educational data needs. The USOE data governance structure centers on the idea that data is the responsibility of all USOE sections and that data driven decision making is the goal of all data collection, storage, reporting and analysis. Data driven decision making guides what data is collected, reported and analyzed.

While data governance works best when all employees take an interest in data and data issues, specific individuals are assigned to guide and facilitate proper data use. Each section at USOE assigns at least one data steward to oversee how data specific to that section is defined, collected, stored, shared and reported. Data does not exist in a vacuum, but is only properly used within context. While Data & Statistics and IT staff have knowledge about data, analysis and data systems, they lack the contextual knowledge needed to make policy decisions about the collection and use of data. Good data management requires both an understanding of the data and an understanding of the program or context. Thus, data stewards function as liaisons and bridge the gap that sometimes exists between "data folks" and "program folks". Data meetings foster collaboration among the USOE sections and between the USOE and Local Educational Agencies (LEAs).

It is important that all data be collected once, have one source system of record, and be shared among all that are authorized and have a need for the data. Reported data should meet the standards of reliability and validity and adhere to established quality control processes. Finally, interpretation and use of reported data should be appropriate to the definitions, the collection, and educational theory surrounding the data.

The following two figures outline the broad data use flow and the overall data governance structure. After which, roles specifically involved in the data governance structure are identified and outlined. Data meetings are also listed and defined. Finally, data flow and data request processes are outlined.

Figure 1:

Data Use Overview

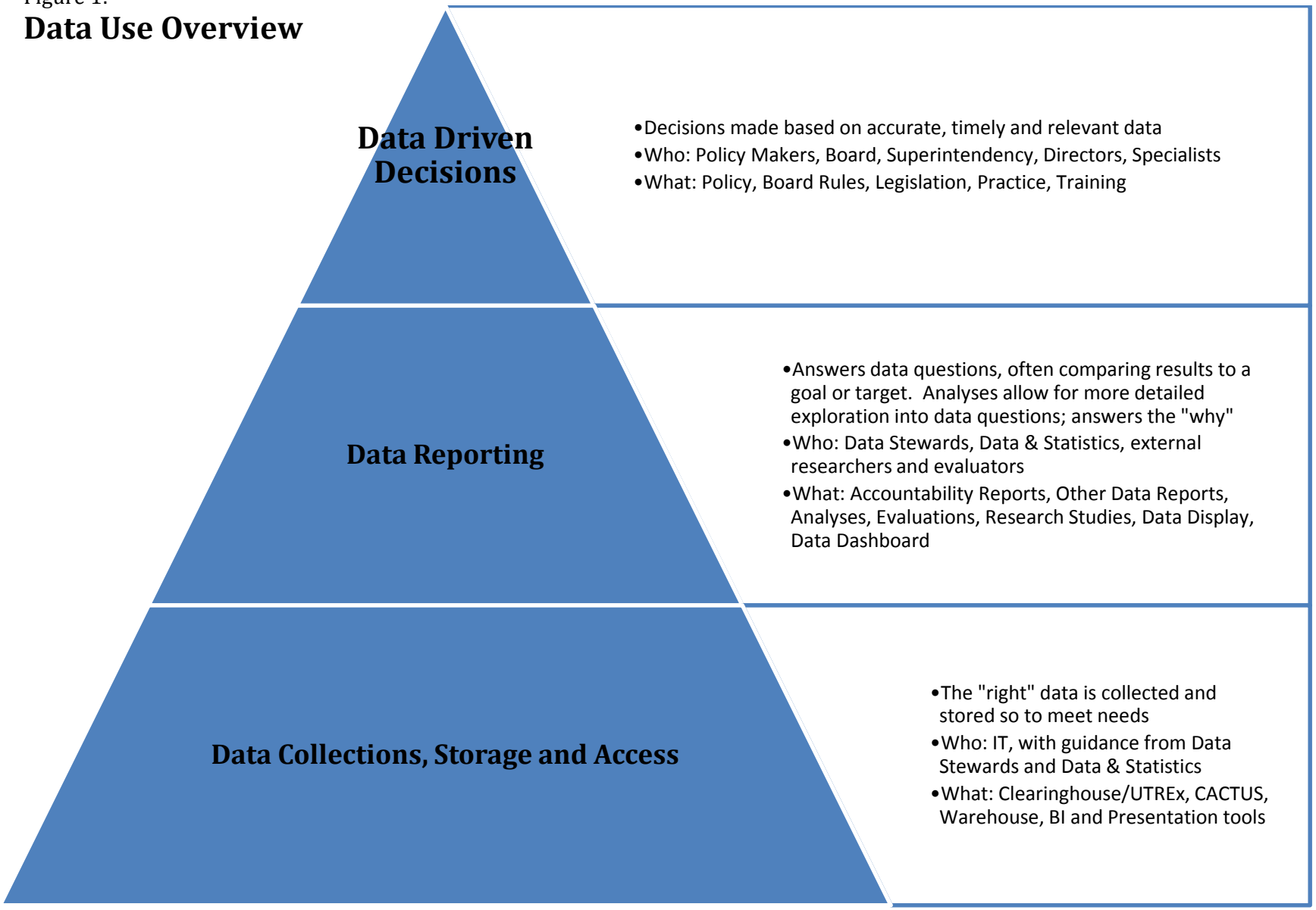
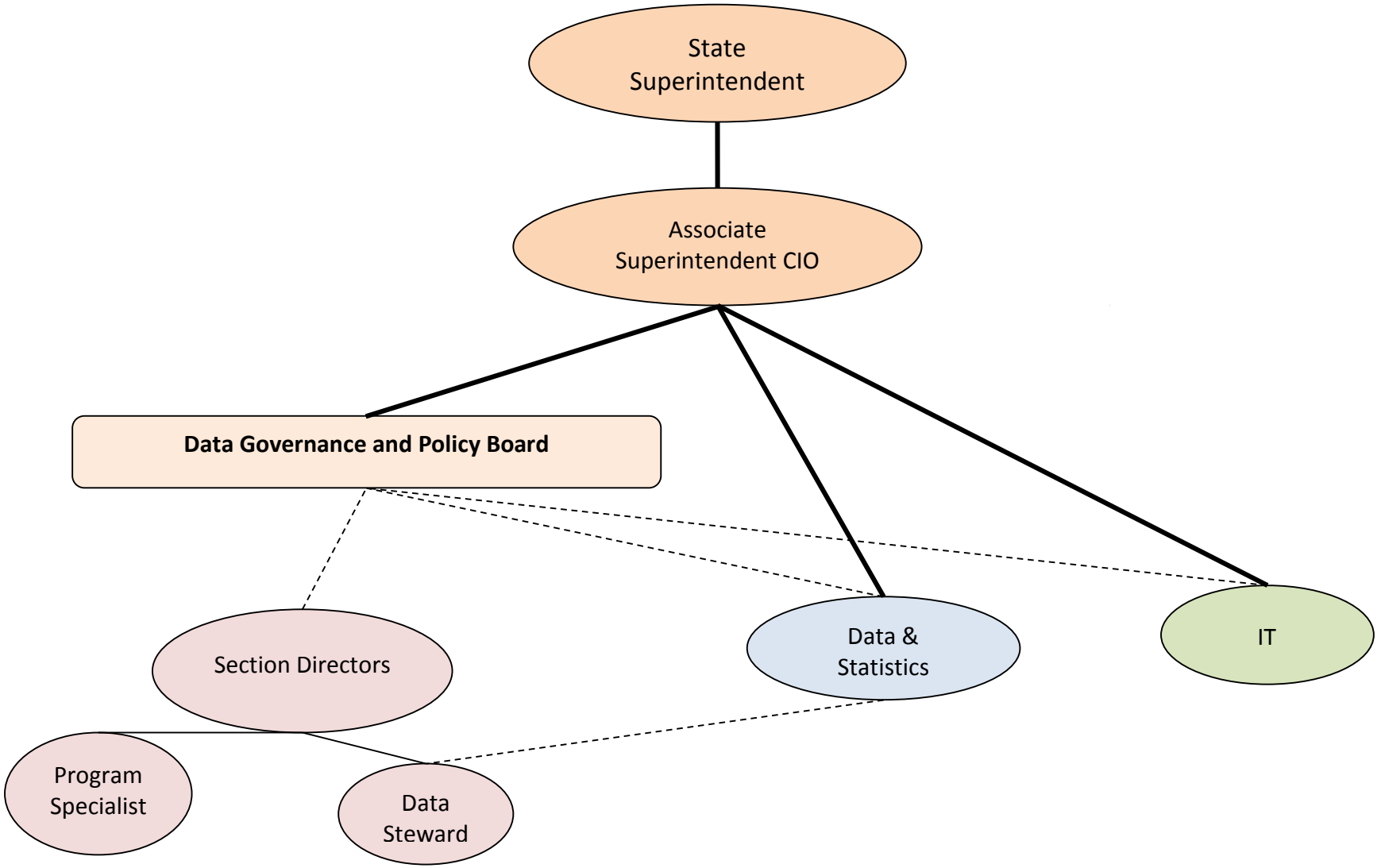


Figure 2:

Overall Data Governance Structure



Data Governance Roles

Associate Superintendent, Student Services and Federal Programs/Chief Information Officer (CIO)

This role is filled by the Associate Superintendent responsible for data reporting, data quality, federal reports and accountability. As CIO, this person is responsible for ensuring that information technology is properly planned for, implemented and effectively maintained to support and enhance business operations and student achievement across all divisions of USOE. S/he also oversees the USOE's technology plan, the management of the organization's data, recommends key technology budget initiatives, provides oversight for the operation and maintenance of the technology infrastructure and applications, ensures proper technology standards are established and followed, monitors service level measures and targets for all technology related support activities, provides project oversight for critical projects and maintains relationships with the local business community and state support agencies.

Data & Statistics Coordinator

The Data & Statistics Coordinator reports directly to the Associate Superintendent over Student Services and Federal Programs. S/he provides leadership for the collection and reporting of data for the USOE. S/he is responsible for the establishing, monitoring, improving and training of the data management and data quality processes and programs for the USOE. In doing this, the Data & Statistics Coordinator coordinates Data Stewards from each section and works closely with IT staff. The Data & Statistics Coordinator also participates in Data Governance meetings in making data policy decisions.

Data & Statistics Section (D&S)

D&S is led by the Data & Statistics Coordinator. D&S fosters collaboration among stakeholders to improve the quality of educational data and to serve the needs of Utah public education; identifies data quality issues and establish and implement policies and procedures to drive accurate reporting of data; defines data presentation and access needs to guide the format of a production layer; produces accurate and timely reports that proactively inform policy and are appropriate to the need and audience; and provide leadership toward innovative data analysis and reporting.

> **Data Analysts**
>
> Data Analysts are part of the D&S section and their task is to improve the quality of the data and to conduct higher level data analyses. Data Analysts perform quality checks data reports, audit data submitted by LEAs, act as data liaisons and build capacity for Data Stewards in data quality. They also conduct major data/statistical projects for the USOE and respond to data needs that span across multiple departments.

Data Stewards

Data Stewards are at the heart of good data governance. They are the link between Data/IT and program areas. Data Stewards are responsible for data content, context, and associated business rules. They must work with D&S and IT to ensure the proper definition, collection, and reporting of the data element for which they are responsible. Data Stewards also must work with their Section Director and Program Specialists in voicing their section's data needs, coordinating data use in their section and responding to data requests from and to their sections (see section on Data Request Process). Each section must appoint a Data Steward to represent that section in terms of data. Data Stewards reside in and are supervised by each section, but are responsible for working with the Data & Statistics Coordinator in discharging their responsibilities. Though an educator license is not required, Data Stewards must have enough program knowledge to understand data

needs, enough authority to make data decisions and function as a data steward, and enough technical/statistical expertise to work with data and understand USOE's data structure.

COGNOS Specialists
USOE currently builds and maintains a data presentation for LEAs that uses COGNOS (called the Data Display). COGNOS Specialists facilitate the use of COGNOS. COGNOS Specialists work with the COGNOS users group and data mentors.

Section Directors
Section Directors are ultimately responsible for data coming from by their respective sections and/or used by them. They assign data stewards. They approve data requests for data owned by their section and data produced by their section. Section Directors attend Data Governance meetings, making data policy decisions.

Program Specialists
Program Specialists' focus on a day to day basis is likely not data. However, Program Specialists are users of data and therefore play an important role in data governance by outlining their data needs and defining data elements for their area. They will do this through their Data Steward. Thus, Program Specialists must work closely with their Data Steward whenever data for their program is being collected or used. They also are responsible for communicating data needs and issues to LEA Specialists and other appropriate external entities. Without input from Program Specialists, data becomes marginalized and less relevant to educational needs and endeavors.

IT Director
The IT Director provides leadership for the planning, implementation and support of information systems, policies and processes for the USOE and works with LEAs on wide-ranging IT initiatives and systems integration. S/He plans and manages the agency technology infrastructure including: computers, printers, firewalls, routers, and dozens of specialized servers with appropriate security, inventory and backup technologies. The IT Director supervises professional IT staff and directs commercial and software acquisitions and development. The IT Director also works closely with the Data Quality Manager in identifying data needs and solutions and participates in Data Governance meetings in making data policy decisions.

Information Technology (IT)
IT does not have a Data Steward, but IT staff works closely with the Data Quality Manager, Data & Statistics and Data Stewards. IT should be informed and a part of all data collections at USOE. IT staff members assist Data Stewards in accessing collected data. IT staff are responsible for the overall agency information technology infrastructure, resources and processes. This includes: all networking hardware and software; all databases and data warehousing; all commercial and custom software applications including their management, development and support; data and IT policies and governance including security, quality and access functions.

MOVEiT Specialists
MOVEiT Specialists are the contact person at USOE for any secure file transfer through MOVEiT. Most often this is a Data Steward or an IT staff member. MOVEiT Specialists certifies that data is applicably transferred and security is appropriately maintained.

Role Matrix Table

Data Governance Activity	CIO	D&S Coordinator	IT Director	Section Directors	Data Analysts	Data Stewards	IT Staff	COGNOS Specialist	Program Specialist
Data Governance									
Establish Data Policy Committees & Boards	X								
Develop Data Governance Policy	X	X							
Approve Data Governance Process	X	X	X	X					
Develop and Approve Data Policy	X	X	X	X					
Assign Data Elements (Stewardship) to Sections	X	X							
Assign Data Elements (Stewardship) within Sections				X					
Identify Data Stewards				X					
Define Data Elements						X			X
Data Reporting									
Identify Research Needs and Data Priorities	X								
Approve Data Requests		X		X					
Respond To Data Requests		X				X			
Work with External Researchers		X			X				
Provide Simple Data Analyses and Reports						X			
Perform More Involved Data Analyses		X			X				
Provide Mechanism for Reoccurring Reports							X		
Quality Check Released Data	X	X	X	X	X	X	X	X	X
Audit Data and Calculations					X	X	X		
Data Collections, Storage, Access									
Identify Data Collection Needs		X		X		X			X
Collect Data							X		
Develop Application Architecture		X	X				X		
Develop Applications							X		
Develop Technology Standards			X						
Define Data Presentation Needs and Elements		X							
Develop/Maintain Data Presentation Framework			X				X		
Develop & Maintain Data Presentation					X		X	X	

Data Governance Groups

Data Governance/Policy Board (DGPB)

Members: Deputy and Associate Superintendents, D&S Coordinator, and all Directors
Meetings: Monthly, Attendance is mandatory
Meeting conducted and facilitated by Associate Superintendent/CIO
Purpose: To resolve the data and process issues and the policy decisions raised by the Data Stewards, the Data Warehouse and CACTUS meetings.

Data Stewards Group Meeting

Members: D&S Coordinator, Data Stewards, Data Analysts, IT Staff, COGNOS Specialists
Meetings: Bi-monthly, Attendance is mandatory
Meeting conducted and facilitated by D&S Coordinator
Purpose: To resolve issues dealing with data reporting, data quality and data processes. Train Data Stewards.

Data Warehouse Group (DWG)/Data Warehouse District

Members: IT Director, IT staff, D&S Coordinator, Data Analysts, Data Stewards, Program Specialists as needed, LEA IT representatives (once a month)
Meetings: Bi-Monthly, Attendance is mandatory
Meeting conducted and facilitated by IT Director
Purpose: To resolve issues dealing with the collection and storing of data in the Warehouse.

Data Technical Meeting

Members: IT staff, D&S Coordinator, Data Analysts, Data Stewards
Meetings: Weekly
Meeting conducted and facilitated by IT and D&S Coordinator
Purpose: To troubleshoot questions about data access.

NAG

Members:
Meetings:

Purpose:

Web

Members:
Meetings:

Purpose:

CACTUS Group Meeting

Members: IT CACTUS staff, D&S Coordinator, Data Stewards as needed, other agency staff working with CACTUS

Meetings: Weekly, Attendance is mandatory
Meeting conducted and facilitated by IT Manager over CACTUS

Purpose: To resolve technical issues dealing with the collection and storing of data in CACTUS.

Data Display Steering Meeting

Members: Assessment Director, COGNOS Specialists, D&S Coordinator, Data Analyst assigned to COGNOS, IT Director, IT Manager

Meetings: Monthly
Meeting conducted and facilitated by Assessment Director

Purpose: To guide direction and purpose of Data Display.

USOE Data and Auditing Group Meeting

Members: D&S Coordinator, Data Analysts, Finance & Statistics Financial Auditors, USOE Auditor

Meetings: *Not yet implemented*
Meeting conducted and facilitated by Data & Statistics

Purpose: To coordinate data auditing efforts. Review auditors' reports. Identify data auditing needs.

District Data Conferences

Members: IT staff, D&S Coordinator, Data Analysts, Data Stewards, applicable Program Specialists, LEA IT representatives, other applicable LEA representatives

Meetings: Twice Each Year, Fall and Spring
Meeting conducted and facilitated by IT Director

Purpose: To coordinate data collections, definitions and practices with LEAs. Inform LEAs of new collections and procedures. Train on data and best practices in handling and using data.

Meeting Matrix Tables

Meeting Participants

Group	Attendees									
	CIO	D&S Coordinator	IT Director	Other Directors	Data Stewards	DQAs	COGNOS Specialists	IT Staff	Program Specialists	Notes
DGPB	L	R	R	R						
DSG		L	O		R	R	R	O		
DWG		R	L		R*	R		R	O	
CACTUS Group		O	O		R*	R		R	R*	
Warehouse Tech		R			O	O	O	R		
Data Conferences	O	R	L	O	R	R		R	O	
Data Display Steering Committee		R	R	R*			R	R		Lead by Assessment & Accountability

L = Leads Group
R = Required Attendee
*R = Required for Relevant Sections
O = Optional Attendee

Meeting Activities

	Group Responsible for Data Governance Activities						
Data Governance Activity	**DGPB**	**DSG**	**DWG**	**CACTUS Group**	**Warehouse Tech**	**Data Conferences**	**Data Display**
Identify data issues		X	X	X	X		X
Develop data governance policy	X						
Sponsor the Data Governance process	X						
Review data reporting policies		X					
Review data collection and management policies			X	X			
Approve data policies	X						
Operationalize data policies		X	X	X			X
Establish working groups to resolve data issues	X	X	X				
Discuss/propose new data collections			X	X	X		
Approve new data collections	X			X			
Review and approve Application Architecture	X		X				
Approve new databases and applications	X						
Develop/review data element standards		X	X	X	X		
Approve data element standards	X						
Develop Technology standards			X	X			
Approve Technology standards	X						
Train on Data Usage		X			X		X

Data Flow

The USOE collects and reports on vast amounts of data. The data flow outlined below creates mechanisms for data collected to be stored and used in such a way as to produce accurate, relevant and timely results. Each layer is important.

Data Collection

Data should be collected once and have one source system of record. Data is collected and received by the USOE through multiple sources. Most student non-assessment data is collected from LEAs through the USOE Data Clearinghouse. There are other data sources, such as state assessment data through the state testing system, educator data through CACTUS, program data collected through mechanisms managed by Program Specialists, and external data such as ACT sent by external entities. While data is collected and received through multiple sources, all data collections and receipts should be supervised by IT.

Formal Collections

Wherever possible, data should only be collected through existing formal collection procedures. Typically, this will mean the Data Clearinghouse. For any new data collections or changes to existing data collections Program Specialists and their Data Steward must work with IT. Ideally, any changes or additions to current data collections must be scheduled a minimum of 18 months before the data is needed. These changes and additions should brought to the Data Warehouse Group meeting as soon as they are known. The section's Data Steward is responsible for working out the details of the collection and its format. Any new data collections or changes to current data collections must be justified, meaning there must be a clear purpose and need for the data.

Ad hoc Collections

While formal collections are norm, there are rare cases when data cannot be collected formally. For example, if a Federal or state mandate requires data that the USOE report data not previously collected and not enough time is given to collect the data through formal collections, an ad hoc collection may be done until the data can be collected through formal collections. No ad hoc collections should be undertaken without support from IT and the section's Data Steward. Further, data from these ad hoc collections should not be stored on an individual's computer.

Data Storage

Data should never solely reside on an individual's computer. Wherever possible, data collected and received by the USOE is stored in a central location, the data warehouse. The warehouse contains longitudinal data from and allows the various collected data to be linked together for a more robust picture of Utah public education. Access to the raw data elements in the warehouse is generally limited to IT. Data Analysts and Data Stewards may have access to the raw data as needed.

Data Access

Data that is collected and stored must be made assessable to all data users in a format ready for data use specific to their needs.

Production Layer

Data tables use the data dictionary to convert raw data into meaningful data sets. The production layer manages the flow of information from the staging part of the data warehouse to an interface that makes it easier for Data Stewards to view and work with the data. The development of this layer is the responsibility of IT and Data & Statistics. Data &

Statistics, with input from Data Stewards, defines the business rules used. Data & Statistics communicates needs to IT, who designs the structure. The presentation layer will draw from the tables created in the production layer. Access to the production layer will be extended to Data Stewards and Data Analysts to develop non-standard data reports and analyses.

Presentation Layer

The presentation layer contains data in a format for easy access and use for general data users. USOE currently builds and maintains a data presentation layer that uses the reporting tool, COGNOS. This layer has been names the Data Display. The Data Display contains dynamic reports that can be used by any educator with very little to no training. The Data Display also contains cubes that allow for more flexibility in data reporting. While cubes are easier to use than the tables in the production layer, they require training and are to be used primarily by Data Stewards.

The Data Display is developed by COGNOS specialists and Data & Statistics, with help from IT.

There are other data presentation tools used by USOE, including static reports in programs such as CACTUS. These are built by IT to fill specific needs for commonly needed reports.

Data Use

There are three levels of data use—strategic data reporting, data analysis and data driven decisions. Data that is strategically measured and then analyzed and/or researched for deeper understanding will lead to appropriate data driven decisions.

Strategic Data Reporting

Strategic data reporting answers many of the "what" or "how many" types of questions. For example, data is reported on how many science teachers are in Utah or if more students are proficient on the Pre-Algebra CRT this year than were proficient last year. Strategic data reporting works best when the data is measured against a goal. Data at this level can be presented in a variety of ways, including a direct answer to a question, a table, a data file, and graphically. The data dashboard and data display present data at this level.

Data at the strategic level is largely the role of Data Stewards. As data stewards reside in program areas, they can provide the contextual knowledge necessary for strategic data use.

Data Analysis

Data analysis goes beyond reporting data. The reported data at the strategic level often leads to further and deeper questions. For example, why did a school not meet a goal or why are a certain group of students improving and others not? These types of questions are addressed by data analysis. At this level analyses are performed to answer the "why" type questions. Analyses are also performed to synthesize and model the data in order to highlight useful trends and correlations and identify other variables impacting results.

While data stewards may do analyses as needed, data analysis and data audits are the responsibility of Data & Statistics.

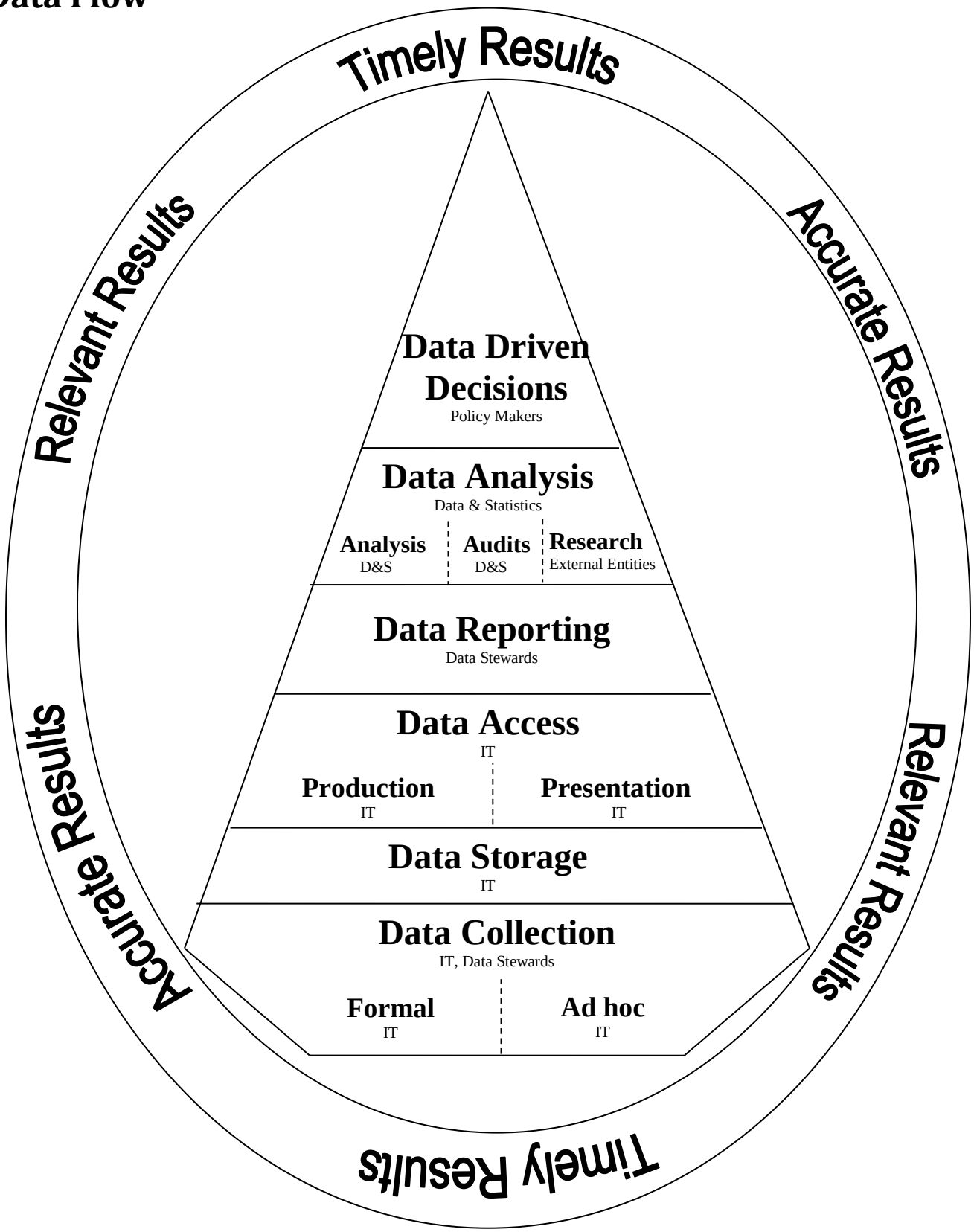
Data Audits
At times the "why" questions leads to questions about the validity and reliability of the data itself. Thus, at this level data audits may be performed to ensure the strategic data reporting is valid. Along with Data Stewards, Data & Statistics is responsible for the quality of the data.

Research
Research is a subset of the data analysis level. Analyses done by the USOE may spark interest for further study that is beyond the scope of the USOE's resources. Thus, it is in the interest of the USOE to work with researchers at Utah Universities and other reputable research institutions to answer these questions.

Data Driven Decisions
Data is not useful unless put into action. Data driven decisions should be the ultimate outcomes of all data collected, stored, accessed and used. Data driven decisions use data from the strategic, analytic and research levels to inform the decision making process for policy changes.
IT, Data Stewards, and Data & Statistics provide the data but do not decide policy. Data Stewards and Data & Statistics guide correct interpretation of the data, but application of the data is a role for policy and decision makers.

Figure 3:

Data Flow



Data Quality

Data quality is achieved when information is valid for the use to which it is applied, is consistent with other reported data and users of the data have confidence in and rely upon it. Good data quality does not solely exist with the data itself, but is also a function of appropriate data interpretation and use and the perceived quality of the data. Thus, true data quality involves not just those auditing, cleaning and reporting the data, but also data consumers.

Data quality at USOE is addressed in six areas.

Data Governance Structure
The USOE data governance policy is structured to encourage the effective and appropriate use of educational data. The USOE data governance structure centers on the idea that data is the responsibility of all USOE sections and that data driven decision making is the goal of all data collection, storage, reporting and analysis. Data driven decision making guides what data is collected, reported and analyzed.

Data Requirements and Definitions
Clear and consistent data requirements and definitions are necessary for good data quality. On the data collection side, the USOE communicates data requirements and definitions to LEAs through the Data Clearinghouse Update Transactions documentation (see http://www.schools.utah.gov/computerservices/Data-Clearinghouse.aspx). The USOE also communicates with LEA IT staff regularly, at monthly Data Warehouse Group meetings and at biannual Data Conferences. Where possible, USOE program specialists are invited to these meetings and the same guidance is given to the appropriate LEA program directors.
On the data reporting side, the production and presentation layers provide standard data definitions and business rules. Data Stewards coordinate data releases through the Data Stewards Group meetings. All data released includes relevant data definitions, business rules, and are date stamped. Further, Data & Statistics produces documentation, trainings and FAQs on key statistics and reports, such as AYP, graduation rate and class size.

Data Collection
Data elements should be collected only once—no duplicate data collections are permitted. Where possible, data is collected at the lowest level available (i.e. at the student/teacher level). Thus, there are no aggregate data collections if the aggregate data can be derived or calculated from the detailed data.
For all new data collections, USOE provides to LEAs clear guidelines for data collection and the purpose of the data request. The USOE also notifies LEAs as soon as possible about future data collections. Time must be given to LEAs in order for them to begin gathering the data needed.
Data definitions and guidelines more clear, respond to district concerns quickly

Data Auditing
Data & Statistics Data Analysts perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with IT and/or LEAs in explaining and/or correcting the anomalies. Data Analysts also work with School Finance to address findings from the Auditors.

Quality Control Checklist

Checklists have been proven to increase quality. Therefore, before releasing data, Data Stewards and Data Analysts must successfully complete the data release checklist in three areas: reliability, validity and presentation. The checklist is as follows.

Reliability (results are consistent)

1. Same definitions were used for same or similar data previously reported **or** it is made very clear in answering the request how and why different definitions were used
2. Results are consistent with other reported results **or** conflicting results are identified and an explanation provided in request as to why is different
3. All data used to answer this particular request was consistently defined (i.e. if teacher data and student data are reported together, are from the same year/time period)
4. Another USOE data steward could reproduce the results using the information provided in the metadata

Validity (results measure what are supposed to measure, data addresses the request)

5. Request was clarified
6. Identified and included all data owners that would have a stake in the data used
7. Data owners approve of data definitions and business rules used in the request
8. All pertinent business rules were applied
9. Data answers the intent of the request (intent ascertained from clarifying request)
10. Data answers the purpose of the request (audience, use, etc.)
11. Limits of the data are clearly stated
12. Definitions of terms and business rules are outlined so that a typical person can understand what the data represents

Presentation

13. Is date-stamped
14. Small n-sizes and other privacy issues are appropriately handled
15. Wording, spelling and grammar are correct
16. Data presentation is well organized and meets the needs of the requester
17. Data is provided in a format appropriate to the request
18. A typical person could not easily misinterpret the presentation of the data

Data Training

Data Stewards meet together bi-monthly at the Data Stewards Group meetings to discuss data reporting and to train on USOE data and good data use. In these meetings (and other ad hoc trainings) Data Stewards train each other about specific data elements (such as definitions, business rules, collections, reports). Data Stewards also are trained on the various data reporting tools (such as SPSS, COGNOS, and InfoMaker) and on good data reporting techniques.

Handling Data Errors

The USOE data governance process minimizes errors in data reporting. However, errors will still exist. Errors in reported data will be handled on a case by case basis, depending upon the circumstance. The impact of the error must be weighed against the impact of correcting the error. The following considerations will guide how to handle any errors in reported data.

Errors in data submitted by LEAs are best found and fixed before collection deadlines
The USOE provides LEAs multiple chances to review and, if necessary, revise their submitted data. Deadlines for data collections are based on reporting timelines. There must be sufficient reason to allow an LEA to resubmit data after a deadline.

Errors are best found and fixed prior to reporting data
Data should be audited and the quality control checklist passed before data is released. There must be sufficient reason revise and re-release data after it has been published.

Accuracy must be weighed with consistency
It is important to provide accurate data to inform policy. In terms of accuracy, it is good practice to revise statistics and reports if an error is found after publishing. This is particularly true if the error may mislead. However, if data errors are corrected after release, the revised data may compete with the previously published data, causing confusion. Changing a calculation so that it is more accurate may also hinder longitudinal comparisons.

Errors made by the USOE in calculating statistics differ from errors in data reported to USOE by LEAs
Errors made by the USOE should not negatively impact schools or districts. There must be sufficient reason to not correct errors made by the USOE if the errors negatively impact schools or districts.

Errors found in current or prior year's data are easier to change than errors from earlier years
The longer the period between the occurrence of the error and the correction, the harder it is to control the effects of correcting the error. There must be sufficient reason to correct errors in older data.

Errors in data used for high stakes decisions (i.e. funding, accountability) are more egregious than other data errors
LEAs should be given opportunities to appeal certain high stakes data, such as that used for AYP. High stakes data that negatively impacts schools or districts should be corrected if possible.

Revisions to previously published data should be clearly documented
Revised reports need to be clearly labeled and explained. Reports should also be date stamped.

Data Requests

Data requests require additional resources to fill. Yet, the benefits of providing data beyond state and federal requirements can outweigh the costs. Providing data to USOE staff helps them in their work. Providing data to persons and entities outside of the USOE increases transparency, promotes education in Utah, and increases knowledge about Utah public education. Thus, the USOE seeks to answer data requests that are relevant to its mission and goals and that benefit Utah public education. Data requests outside this scope can only be accommodated when resources are available.

The following four charts (figures 4-7) outline the data request process. Figure 4 shows the overall workflow, as described below. Figures 5-7 show the request process after the workflow has been assigned.

Data requests are largely the duty Data Stewards, but are supervised by the Data & Statistics Coordinator. There are three types of requests, each handled differently:

Internal Data Requests
All requests made by USOE employees should be made using the Data Request Form on SharePoint (http://intranet/sections/DATA/DSG/Lists/Data%20Requests/Default.aspx). This form automatically assigns the request to the appropriate Data Steward and allows for the tracking of all internal data requests. Internal data requests are approved by the department making the request and are filled by that department's Data Steward.

External, Non-Confidential Data Requests
Requests made by persons or entities outside of USOE for non-confidential data are handled by the sections responsible for the data requested. Such requests can be entered into the Data Request Form on SharePoint by a USOE employee. They may also be initiated by the requestor completing the web request form on the USOE website under Data & Statistics, Educational Data, Data Requests (http://www.schools.utah.gov/main/DATA-STATISTICS/Educational-Data/Data-Requests.aspx). If a single department is responsible for all the data requested in the external request for non-confidential data, the request is approved and handled solely by that department. If the non-confidential external data request covers multiple departments, it handled by the Data & Statistics Coordinator who assigns parts of the data requests to the appropriate Data Steward(s). (For an outline of what is non-confidential data, see the section on Permitted Disclosures.)
USOE will charge $60/hour for time spent on eternal data requests beyond two hours. For Utah universities, students attending Utah Universities and Non-profit Organizations, USOE will charge $60/hour for time spent on eternal data requests beyond four hours. Fees may be waived on a case by case basis.

External, Confidential Data Requests
External data requests for confidential data protected by FERPA must complete the Researcher Data Request form and agree to and sign a Confidentiality and Use Agreement. These requests are handled by the Data & Statistics Coordinator, who will draw assistance from the appropriate Data Stewards and IT staff to fill the request. Before USOE will enter into an agreement to release confidential or protected data the relevant department(s) must approve the request and agree to sponsor the request. As the sponsor, a department will certify the benefit to USOE and its mission, field questions from the requestor, and assist the Data & Statistics Coordinator and IT staff in filling the request.
USOE will charge the same amount as for external, non-confidential data requests.

Figure 4:

Data Request Overall Workflow

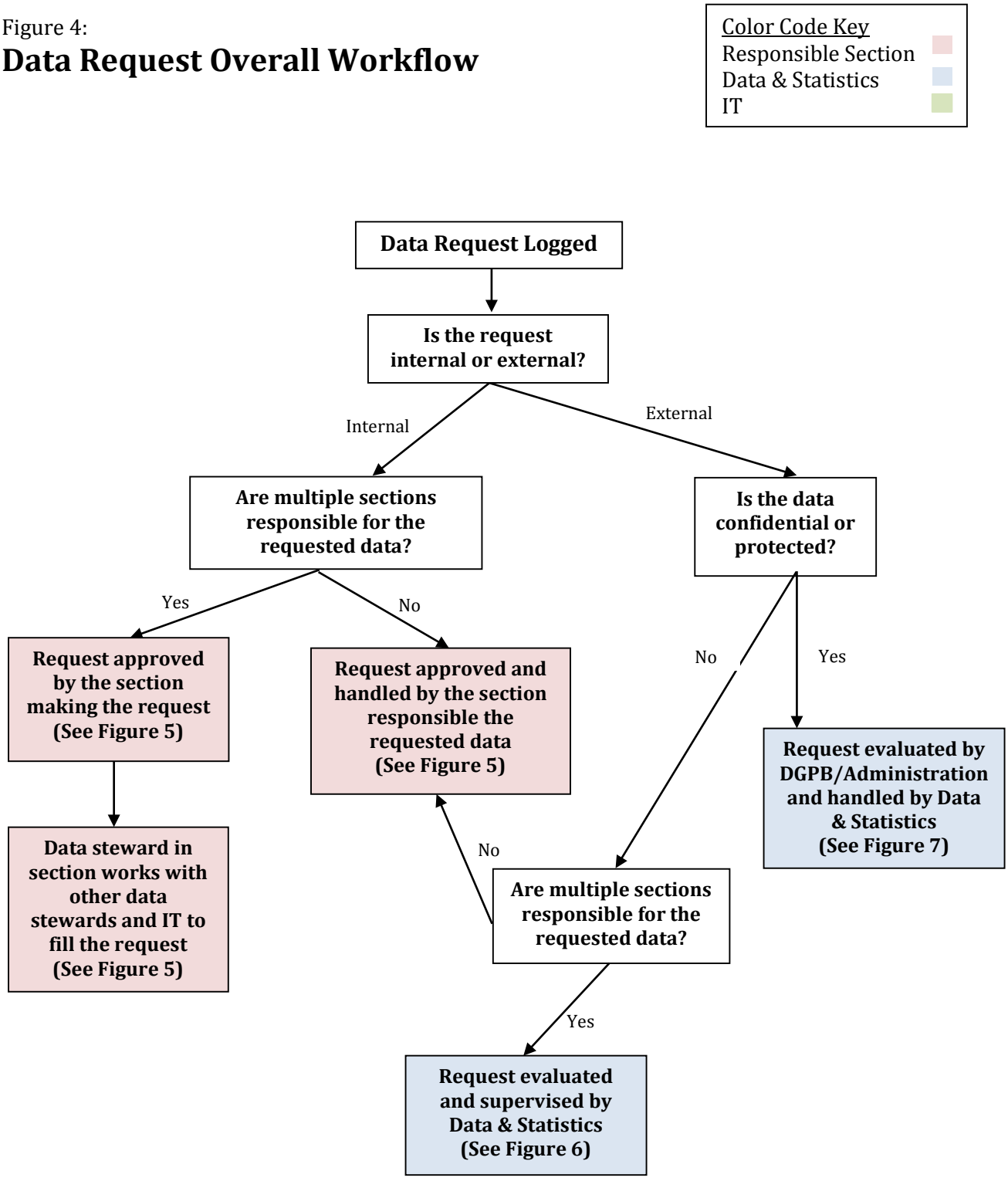


Figure 5:

Data Requests Handled by a Single Section

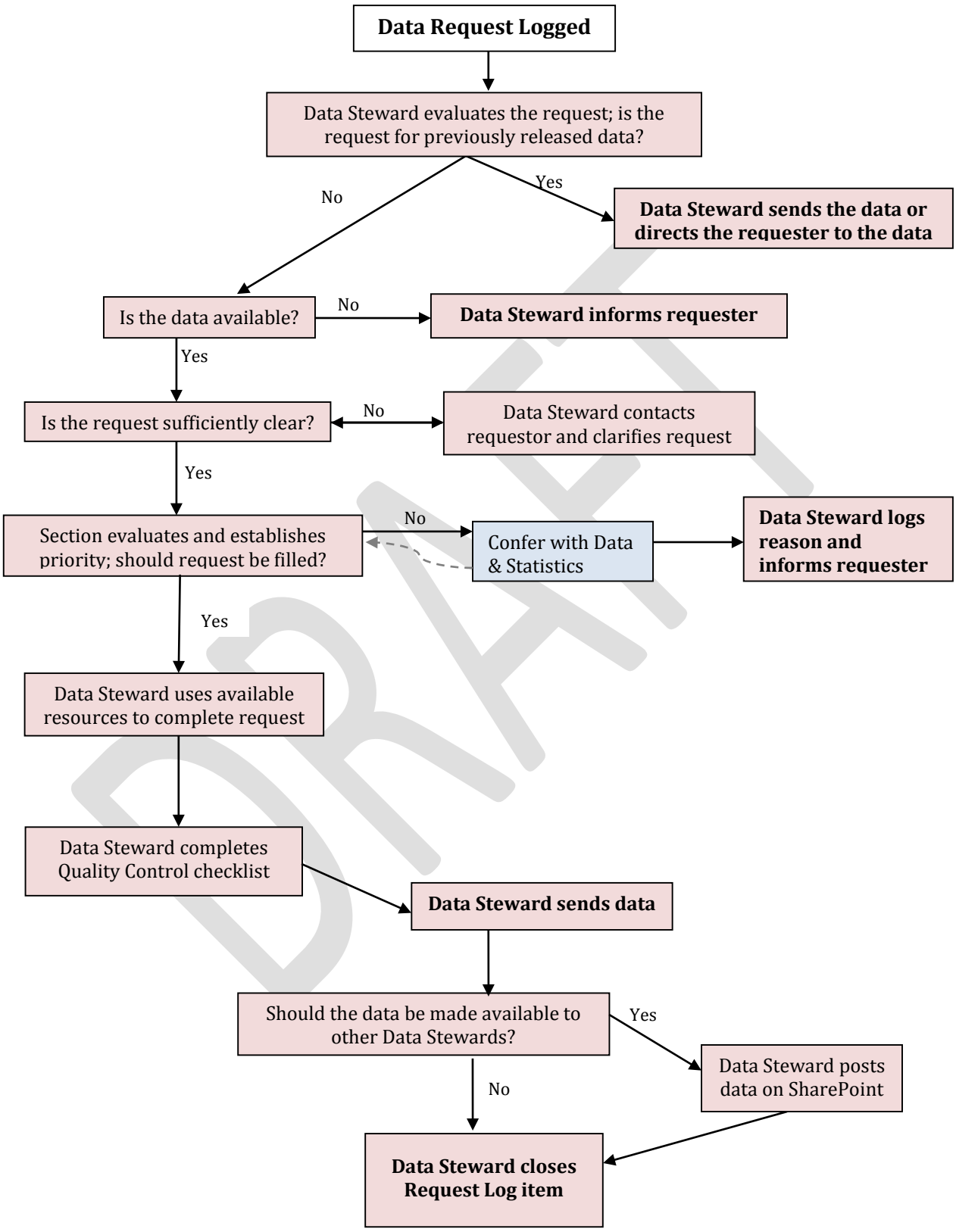


Figure 6:

External, Non-Confidential Data Requests for Data from Multiple Sections

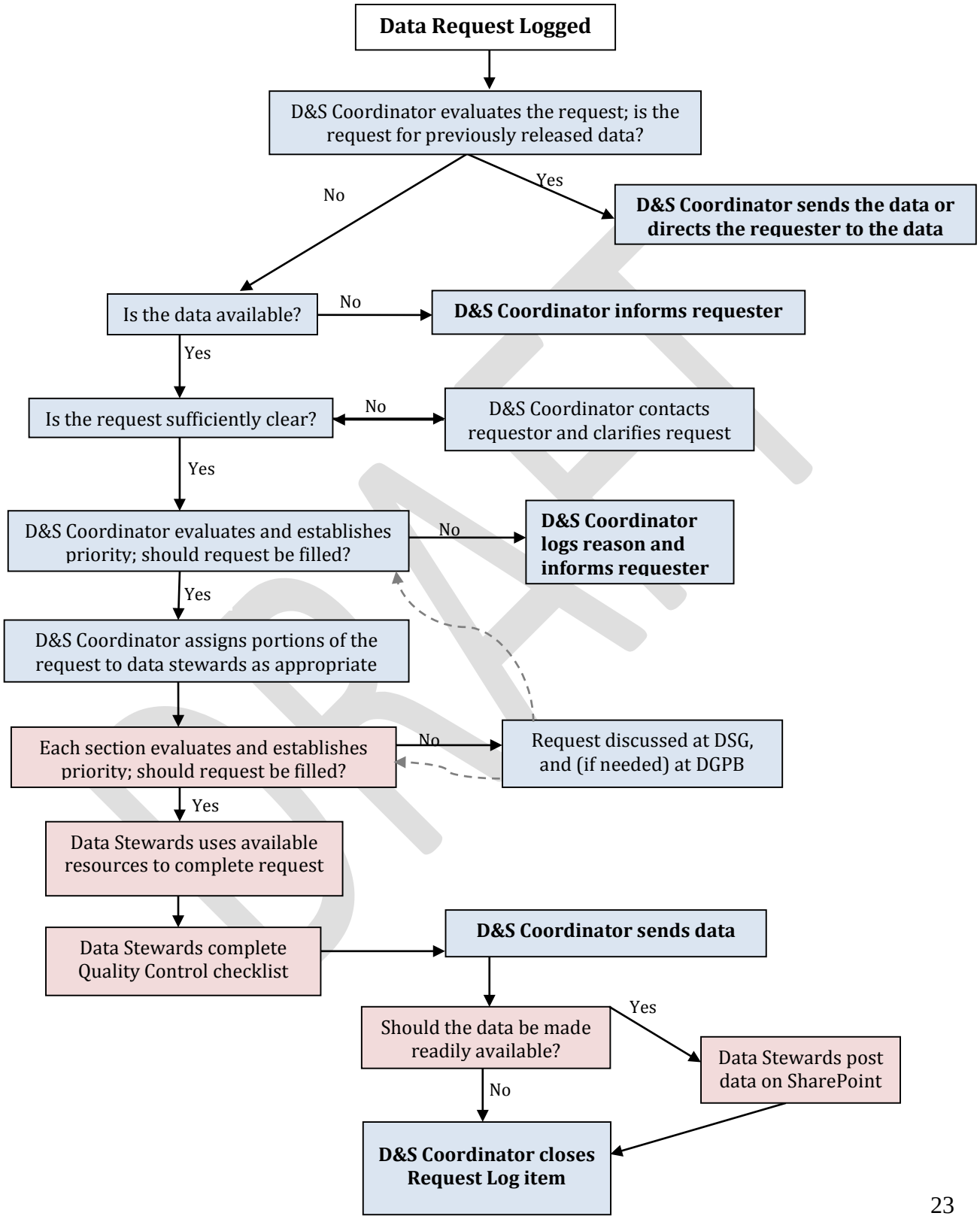
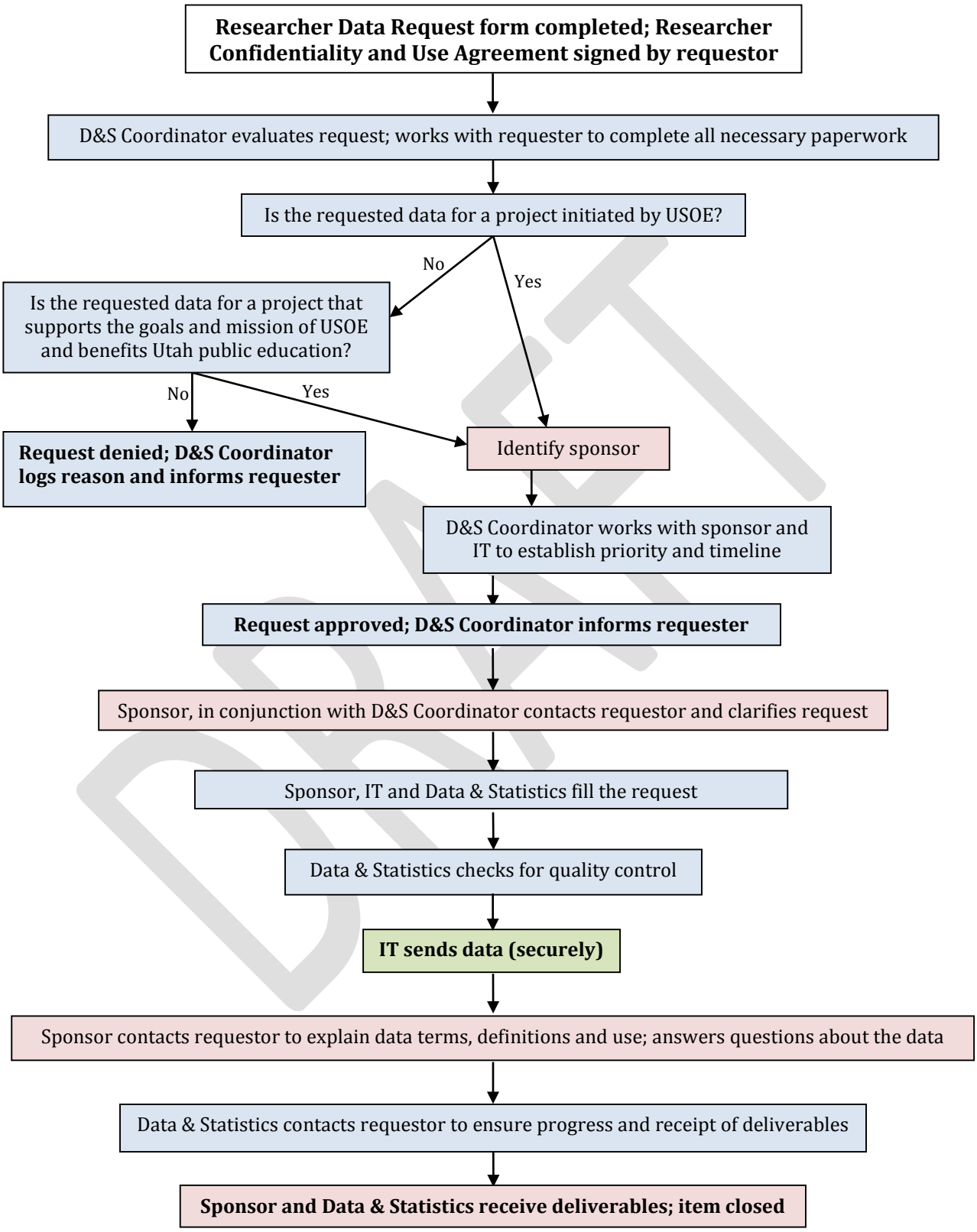


Figure 7:

Confidential or Protected Data Requests



Permitted Disclosures

Certain data is protected and cannot be released. Data on students is governed by FERPA and data on educators is governed by GRAMMA and USOE policy.

Student Data

With student data there are three questions to consider.

1. Is the requested information "directory information?" Directory information is defined by local districts and may include name, phone number, address, date of birth, awards, honors, activities the student participates in, photographs, videos of students.
    - All directory information may be released without prior written parental or student consent.
2. Is the requested information an education record? Education records are records, in any format, created and maintained by the education agency that directly relate to a student. A state superintendent report on education is not an "education record;" a student's score on a state CRT is.
    - Education records may not be released unless the information falls under an exception.
3. Is the information identifiable? Personally identifiable information includes a student's name, the name of the student's parent or other family member, the address of the student or student's family, a personal identifier such as the student's social security number or student number, a list of personal characteristics that would make the student's identity easily traceable, or other information that would make the student's identity easily traceable. USOE considers district and school name to be PII at the student level. USOE does not consider the above characteristics PII if aggregated where the n size is greater than 10.
    - If a reasonable researcher could determine who the student is based on the information, it may not be released unless the information falls under an exception. The USOE does not release data where the n size is less than 10 or if a larger group is 0 or 100 percent.

In general, if the requested information is part of an education record or if the requested information contains identifiable information that is NOT included in the definition of directory information, it can ONLY be released with parental consent or if one of the exceptions to consent applies.

If the answer to any of the following questions is "yes," the information may be disclosed with proper logging of whom requested the information, when it was released, what information was disclosed, and a written reminder (in the form of a cover letter or written agreement, depending on the situation) to the requester that the information may not be disclosed to a third party and must be destroyed within a specified time period.

1. Is the requestor a school official who has a legitimate educational interest in the child? Example of an acceptable use NOT requiring parental permission: The school principal asks to see the test scores of five students over the past ten years to determine proper placement.
2. Is the requestor from another school, school system, or post-secondary institution where the student seeks or intends to enroll? Example of an acceptable use NOT requiring parental permission: The student sent an application in to a private school. The school requests the student's test scores as part of the application process.
3. Is the requester from the Dept. of Education, comptroller general of the United States, or a state or local education authority?

- Is the requestor seeking the information as part of an audit or evaluation of federal or state education programs? OR
- For the enforcement of or in compliance with requirements related to those programs?

4. Example of an acceptable use NOT requiring parental permission: The Dept. of Ed. requests student level information for charter schools as part of its evaluation of our use of Race to the Top funds.
5. Is the requestor conducting a study "on behalf of" USOE? "On behalf of" means USOE agrees with the purpose of the study (though it may disagree with the results) and retains control over the information from the education records that it disclosed.
    - is there a written agreement between USOE and the researcher specifying the purpose of the study, AND
    - is the purpose (A) related to the development, administration, or evaluation of predictive tests, or (B) related to the administration of student aid programs or (C) to improve instruction, AND
    - does the agreement specify the scope and duration of the study, AND
    - does the agreement require that the researcher destroy or return all of the personally identifiable data when it is no longer needed and specify a time period for the destruction or return of the information?
6. Is the requested an accrediting organization seeking information for the accreditation process?
7. Is the requester a custodial or non-custodial parent of the student?
8. Is the request in the form of a valid judicial order or subpoena? You may provide the information but must make reasonable efforts to inform the parents of the subpoena or judicial order.
9. Is the request made to protect the health or safety of a student or other individual? Example of an acceptable use NOT requiring parental permission: A police officer asks USOE which school a student is enrolled in as part of an effort to locate a missing child.

Educator Data

GRAMA requires that we release educators' work contact information and qualifications for licensing. Most aspects of the CACTUS record are considered public record and are available to individuals requesting the information. This includes license status, endorsements, degree information, current assignment, business email, address and phone number, etc.

Educators' ethnicity, birth date, personal email, and home addresses are private and protected information and may NOT be released to third parties. USOE employees may use the private data fields for essential research within the agency if

- There is a compelling reason to use the data that is related to our core functions, AND
- Any released information using these private data fields are not identifiable.

USOE Information Technology Security Plan

1. Introduction.

This document, along with appendices, is a detailed description of security practices within the USOE. It is meant to be a dynamic plan that will, at least in part, be shared will all staff through appropriate training and media. Some of the information presented in this plan was borrowed from public sources, most notably the National Center for Education Statistics (NCES) web site (http://nces.ed.gov).

2. Security Management Processes

At the present time oversight of security a the USOE is quite decentralized with no designated security officer. Work is in progress to change this situation in the future. Although there is no dedicated security office at this time most of the practices and activities below are being conducted by various staff in their currently assigned roles. Two areas in which implementation are not complete the present time are in training, intrusion detection and to some extent qualify assurance. If a fulltime security office were present the would also:

2.1. Communicate to staff that protecting the system is not only in the organization's interests, but also in the best interest of users.
2.2. Increase staff awareness of security issues.
2.3. Provide for appropriate staff security training.
2.4. Monitor user activity to assess security implementation.
2.5. Be inclusive when building a security and contingency planning team by including:
  2.5.1. Key policy-makers
  2.5.2. The security manager
  2.5.3. Building management
  2.5.4. Technical support
  2.5.5. End-users
  2.5.6. Other representative staff
  2.5.7. Local authorities
  2.5.8. Key outside contacts (e.g., contractors and suppliers)

3. Physical Security

3.1. Building
  3.1.1. Fire Projection. The building is protected by a fire detection system.
  3.1.2. Building access. All external doors, but one, are locked at all times and require an electronic key for entry.
  3.1.3. Onsite Guard. One door is unlocked during business hours (7:00 AM to 5:30 PM) and monitored by a guard
  3.1.4. Surveillance cameras. The guard, during business hours, also has access to external and internal surveillance cameras.
  3.1.5. Internal Building Access. After business hours all sections of the building except the main first floor hallway are also secured. The computer services section is in the basement of the building to which access is denied to all but authorized employees during non-work hours.
  3.1.6. Employee Building Access. Employees are screened and given off hours access to appropriate areas of the building depending on their roles. All employees must wear USOE badges at all times within the building.

3.2. Network Room

3.2.1. Water damage. All hardware is elevated off floors in racks of some sort. Likewise for wiring. The fire prevention sprinkler system is dry loaded (no water immediately overhead), meaning that water can only be released if an actual fire triggers a valve behind the actual sprinkler system.

3.2.2. Physical Access. Only one inconspicuous door provides access to the network room and that door is secure by a key pad lock.

3.2.3. Electrical Overloads. Hardware VA rating and totals are assessed to make sure any one circuit is not overloaded. When needed, more circuits are added to the network room. Total volt-amps and wattage is kept at 60% or lower of maximum capacity of a circuit.

3.2.4. Earthquakes. Individual devices are securely attached to racks and racks are anchored to ceiling, floor or other secured racks.

3.2.5. Power Backup. All network room hardware is on UPS and all UPS are on a diesel powered generator backup power system which is able to supply emergency power to the building for at least 24 hours.

3.2.6. Temperature control. If the temperature climbs past a predefined maximum, currently 76 degrees Fahrenheit, automatic alarms are trigger and automatic phone calls are made to key USOE computer services staff and state DFCM (Division of Facilities and Construction Maintenance).

3.2.7. The HV/AC system is also on diesel powered generator backup. When power is lost to the building the air conditioning continues to function for up to 24 hours by running off the diesel generated power. Without continuous air conditioning the heat generated by the electronic equipment would quickly cause the temperatures to rise to levels which would be hazardous to the electrical equipment.

4. Data/Information Security & Privacy/Confidentiality (see APPENDIX A for more details about privacy, FERPA and GRAMA at the USOE)

4.1. Confidentiality. The federal Educational Rights and Privacy Act (FERPA) has an overriding influence on the management of data and information systems at any local or state level public education agency. In fact, like its financial institution's counterpart, Sarbanes-Oxley, FERPA either directly or indirectly drives much of what is contained in this security plan. Whereas Sarbanes-Oxley directly prescribes stringent financial controls and therefore indirectly a myriad of technological security measures, FERPA demands strict controls over the maintenance and use of student data.

4.2. Other Important Privacy and Confidentiality needs. Besides FERPA, the USOE is also responsible for providing controls over processes and procedures around educator licensing data, rehabilitation systems and records as well as school funding, budgeting and financing records and systems.

4.3. FERPA Overview. The federal Educational Rights and Privacy Act (FERPA) of 1974 which has been amended 29 times to date (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education FERPA Fundamentals. See: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

4.3.1. Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

4.3.2. Schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions

4.3.3. School officials with legitimate educational interest;

4.3.4. Other schools to which a student is transferring;

4.3.5. Specified officials for audit or evaluation purposes;

4.3.6. Appropriate parties in connection with financial aid to a student;

4.3.7. Organizations conducting certain studies for or on behalf of the school;

4.3.8. Accrediting organizations;

4.3.9. To comply with a judicial order or lawfully issued subpoena;

4.3.10. Appropriate officials in cases of health and safety emergencies; and

4.3.11. State and local authorities, within a juvenile justice system, pursuant to specific State law.

4.3.12. Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

4.4. FERPA and USOE. The USOE collects massive and detailed amounts of data from schools each year including data about individual students within the Utah public education system.

4.4.1.

Although these data are necessary for accurate state and federal accountability reporting, many of these data sets are essentially “on loan” from the individual school districts of Utah. Usually only the districts ever release such data to outside parties. Therefore the USOE does not, as a general rule, ever release a district’s student level data unless it is back to the originating/owning district or to a research entity that has been granted permission by the district(s) involved. The federal government does not receive individual student level data, just aggregates of some sort.

4.4.2. Except for the Statewide Student Identifier (SSID) system the identity of a student is masked as much as possible. No names are associated and

linking identifiers or keys have been encrypted to prevent such linking and identification of individual students from the district accessible SSID system.

4.5. Data/information integrity (preventing unauthorized creation, modification, or deletion of information):

4.5.1. USOE staff is never to send sensitive information as e-mail. If e-mail absolutely must be used, the file is to be encrypted and sent an attachment rather than in the text of the e-mail message.

4.5.2. Where at all possible all data are to be encrypted before it leaves a server or workstation.

4.5.3. Secure FTP and SSL are always to be employed when transmitting data to and from district facing applications

4.5.4. All data encryption devices and keys are to be physically protected. They must be stored away from the computer.

4.5.5. All staff are to be informed that all messages sent with or over the organization's computers belong to the organization and therefore subject to monitoring.

4.5.6. The receiver's authenticity must be verified before sending any USOE housed information. Everyone sending data outside the agency must ensure that users on the receiving end are who they represent themselves to be by verifying: 1) Something they should know-a password or encryption key; this is the least expensive measure but also the least secure or 2) Something they should have-for example, an electronic keycard or smart card.

4.5.7. Likewise, all data senders need to consider setting up pre-arranged transmission times with regular information trading partners: If you know to expect transmissions from your trading partners at specific times and suddenly find yourself receiving a message at a different time, you'll know to scrutinize that message more closely.

4.5.8. Likewise everyone must maintain security when shipping and receiving materials: When sending sensitive information through the mail, or by messenger or courier, require that all outside service providers meet or exceed your security requirements.

4.6. Practice the following safe data storage:

4.6.1. Backup files require the same levels of security as do the master files (e.g., if the original file is confidential, so is its backup).

4.6.2. Clearly label disks, tapes, containers, cabinets, and other storage devices: Contents and sensitivity should be prominently marked so that there is less chance of mistaken identity.

4.6.3. Never store sensitive information in such a way that it commingles with other data on floppy disks or other removable data storage media.

4.6.4. Information, programs, and other data should be entered into, or exported from the system only through acceptable channels and by staff with appropriate clearance.

4.6.5. Write-protection should be used to limit accidental or malicious modification of files. Note that while write-protection is effective against some viruses, it is by no means adequate virus protection in itself.

4.6.6. Train staff to promptly notify the system administrator/security manager when data are, or are suspected of being, lost or damaged.

4.7. Dispose of Information in a Timely and Thorough Manner:
  4.7.1. Follow all USOE and State of Utah retention schedules for specific information or data sets.
  4.7.2. Mark files to indicate the contents, their expected life cycle, and appropriate destruction dates.
  4.7.3. Before discarding or surplusing obsolete or old media, it will be scrubbed or overwritten to make data recovery impossible. CD ROMs will be physically shredded.
  4.7.4. Consider degaussing (a technique to erase information on a magnetic media by introducing it to a stronger magnetic field) as an erasure option.
  4.7.5. Burn, shred, or otherwise physically destroy storage media (e.g., paper) that cannot be effectively overwritten or degaussed or scrubbed.

4.8. Data Availability: Where data access is permissible the USOE must prevent any unauthorized delay or denial of information to qualified parties. Strict adherence must be given to FERPA and GRAMA at all times.

5. Software Security

5.1. Software installation. Only network administrators and power users (see Appendix B) have rights to install or otherwise add software to any desktop or notebook systems. Only network administrators can install or add software to servers. For a list of software. (see APPENDIX C and APPENDIX D.

5.2. Storage of master copies. Master copies of all software, licenses and documentation are retained in a secure location within the secure network room. Spreadsheets of licenses are maintained along with expiration and renewal schedules.

5.3. Approved Software. Only USOE Computer Services approved and purchased software (see Appendix C) that is installed by USOE network staff or USOE power users may be installed on USOE machines. With permission, power users may install individually purchased copies of software acquired personally or through their UOSE section. However, they must have licenses for all such software available at all times.

5.4. Non-Computer Services approved and purchased software. Before permission will be given to a power user for the installation of any non-CS approved software the user must submit a written request describing the nature of such software and the purpose for which it is to be installed.

5.5. Monitoring of software. To counter possible copyright infringements caused by unlicensed software on organizational equipment that puts the entire organization at risk for fines and other penalties stemming from copyright violations, software inventories will be done on a regular basis. These comprehensive network-wide inventories will include the: the product, name of the manufacturer, version number, and the computer on which he software is installed. This inventory will be reconciled against the Computer Services software license inventory to verify that no unlicensed software or software for which the USOE has inadequate licenses is installed anywhere on the system.

5.6. Train staff on software use and security policies. The best designed software for accessing and manipulating information is useless if staff are unable to use it properly. In conjunction with human resources, Computer Services should prepare and conduct software and technology awareness workshops.

5.7. Regulate Software Development and Changes:

5.7.1. Software development life cycle. All custom software is developed following a strict software development life cycle. (see APPENDIX E)

5.7.2. Authorization of software changes. Before anyone modifies or creates any software, a formal, written change request (see APPENDIX F) must be submitted to the IT director or an IT manager. Such requests must be signed by a section director or associate superintendent and result in an audit trail of artifacts and events as the request is processed.

5.7.3. Design Reviews. Continued feedback is expected from users during the software development process to ensure that the new or changed software will satisfy functional specifications and security requirements.

5.7.4. Production vs. Development Copies. To avoid putting active applications and files at risk all new development is done in a separate development/testing environment with separate test networks and servers were applicable. Once the modified or new copy/version of the software is thoroughly tested by the software development staff and prospective end-users, then and only then will it be deployed to the production or "live" environment.

5.7.5. Program review. Before new or changed programs are put into production the code changes are reviewed by at least one other person who understands the change request that initiated the new or changed code. This step, of course, precedes actually testing and is just one step in the quality assurance/quality control process.

5.7.6. Vulnerability checking: As much as possible program code should also be reviewed and tested for potential vulnerabilities such as buffer overflows and SQL injection attacks that would make it susceptible to various software exploits.

5.7.7. Master files. Master files of all developed software are maintained independently of the development staff: Software belongs to the organization, not the programmer. All original copies are controlled and the organization clearly guarantees this ownership. Require that any new or modified software be tested rigorously and certified as fully operational before releasing it for general use. (see APPENDIX G)

5.7.8. Required documentation. For all new or revised programming, requisite documentation includes among others: the name of the developer, the name of the system, the modules/objects impacted, programming languages/technologies, the development/change dates, nature of the revision, the revision number etc.

5.7.9. Public programs: If software downloaded from the Internet must be used with sensitive information, be sure that it has not been tampered with by checking for a digital signature to verify its authenticity.

5.7.10. Software Verification: Before putting the software into operation, verify that all software user functions are working properly. Check that new software meets anticipated user needs, current system requirements, and all organizational security standards. This recommendation is also applicable when upgrading software.

5.7.11. Upgrade backups: Before installing new software or software upgrades: The latest copies of data files bust be backed-up until the new software or upgrade is proven to be and running properly.

5.7.12. Application software testing: Never risk losing live data with newly installed software. Always run dummy files and/or copies of non-sensitive files through the software to verify software's integrity and proper functioning.

5.7.13. Test machine isolation: Initial software testing should occur on test machines and a test network if at all possible. By maintaining a separate test environment, the entire system is not at risk if the software malfunctions.

5.7.14. Parallel software testing: Run old software at the same time and with the same data as the new software. It should be confirm that the new versions of the software must generate the same results as the existing system.

5.7.15. Backup of Custom Software: Like all other data on USOE servers all custom developed software including commercial software that has been modified with permission is backed up on a predefined schedule. See backup plan in section 6.4.

6. Data Access Security*:*

While the vast majority of system users are trustworthy, there are occasional computing accidents. Most system problems are the result of human error. By instituting security procedures, the organization protects not only the system and its information, but also each user who could at some point unintentionally damage a valued file. By knowing that "their" information is maintained in a secure fashion, employees will feel more comfortable and confident about their computing activities.

6.1. Passwords: After an independent audit of our agency it was recommended that we take this action to improve security. The majority of our password database was cracked within 3 seconds. This is why the new password policy is being implemented. Here is a more precise definition of a strong password.

6.1.1. All passwords be at least eight characters in length (ten or more is preferable).

6.1.2. No passwords are permitted that are words, names, dates, or other commonly expected formats.

6.1.3. Passwords should not reflect or identify the account owner (e.g., no birthdates, initials, or names of pets).

6.1.4. The password character string must contain one character from three of these four character types:

6.1.4.1. Uppercase letters

6.1.4.2. Lowercase letters

6.1.4.3. Numerals

6.1.4.4. Non-alphanumeric characters such as: (, . ; : * % &)

6.1.5. All users are forced to change passwords at least once every 90 days.

6.1.6. No users may share passwords.

6.1.7. Unsecured storage of personal passwords is forbidden (e.g., they should not be written on a Post-It™ note and taped to the side of a monitor).
6.1.8. A password may never be used as part of an e-mail message.
6.1.9. Users should be warned not to type their password when someone may be watching.
6.1.10. Mask (or otherwise obscure) password display on the monitor when users type it in.
6.1.11. Remind users that it is easy to change passwords if they think that theirs may have been compromised.
6.1.12. No new password may be the same as an old password unless at least four other unique passwords have been used in between.
6.1.13. Users are discouraged from using the same password for two or more systems.
6.1.14. There have been questions about people wanting to keep their passwords the same across multiple systems such as: BASE, CACTUS, local network, PATI, AIMS, and IRIS. This is not a recommended practice. If your password were the same across multiple systems then a hacker who cracks one password would be able to access all of the other systems as well.
6.1.15. Mainframe passwords must also start with a letter, no special characters are allowed and all letters must be lowercase. Examples of passwords that will work are: syracuse1, and gr8dane.

6.2. Remote Access: Pre-approval must be given to all remote access privileges: All users must abide by a strict network access policy (see APPENDIX J) that governs attachment of individual computers both at home and at the workplace.

6.3. Walk-in/Guest users: Any walk-in or guest user must abide by the policies set forth above.

6.4. VNP Connections: All connections made through VNP (Virtual Private Networking) by telecommuters or wireless users within the building must be made through agency owned and maintained machines. These machine will be allowed access only through MAC address identification.

6.5. Remote Access Monitoring: Staff must be reminded that remote access is particularly subject to monitoring activities. Increased risk requires increased vigilance.

6.6. Message Authentication: Use software that requires "message authentication" in addition to "user authentication": Even if a user can provide the right password, each message sent and received must have its delivery verified to ensure that an unauthorized user didn't interrupt the transmission.

7. Network Security:

An "access node" is a point on a network through which you can access the system. If even one such point is left unsecured, then the entire system is at risk. All modular jacks and wireless base stations represent potential nodes to which a computing device could be attached.

7.1. Protection of cables and wires: All cabling and wires should be protected as much as possible. This means they should reside in trays in cubicles or within walls or ceilings. If a sophisticated intruder can access a span of cable that is used as a connector between pieces of equipment, he or she may be able to access the entire system.

7.2. Boot secured servers: Secure all servers so they cannot be booted from removable devices or their bios altered with administrative access.

7.3. Screen savers: Screen savers with mandatory locking features must be installed on all user machines to prevent information from being read by anyone who happens to be walking past the display monitor. They should be set to activate after no more than 10 minutes on inactivity.

7.4. Firewalls: Firewalls must be installed at all external access points: Only allow trusted (authenticated) messages to pass into your internal network from the outside. Only predefined ports may be opened.

7.5. Intrusion detection: In conjunction with its firewalls, the USOE will maintain intrusion detection software running in an appropriate configuration but probably within the firewall's demilitarized zone (DMZ). Such software will detect possible intrusions, hacks, or other exploits aimed at compromising the system.

7.6. Modems: Only in very special cases should a modem be necessary. There is no need to provide a viable line of access to and from the system unless it's absolutely necessary. A modem could provide just such access.

7.7. Internet Access: Internet access should be granted to only those employees who need it to perform their jobs. More and more staff are finding useful, job related, services on the internet. However, some job functions may not require it.

7.8. Job related sites: Remind all users that the Internet (and all system activity for that matter) is for approved use only: There are countless Internet sites and activities that have no positive influence on the public education environment.

7.9. Acceptable use policy/agreement: All users are required to sign the USOE's acceptable use agreement before receiving access to the network. Signed and filed acceptable use agreements (see APPENDIX I) verify that users have been informed of their responsibilities and understand that they will be held accountable for their actions.

7.10. Placement of Resources and Firewall: All equipment and information that is intended for external users must be located outside of the firewall or in a DMZ sub-network:

7.10.1. The USOE's public Web servers that are intended to provide information and services to the public must be located in such a DMZ. Such Web servers must not be able to access confidential information that resides inside the firewall. This way, if the public Web server should ever be compromised, confidential information is still protected. All development for

such Web servers must take place within a testing environment within the network.

7.10.2. After testing, public web pages are published to a staging Web server inside the firewall that continually synchronizes or updates the production Web server outside the firewall. If the public Web server ever fails it can be quickly be rebuilt from this staging Web server.

7.11. Protection of transmissions Sent over the Internet:

7.11.1. SSL: Secure Sockets Layer (SSL) Servers must be used to secure all private information transactions made with a Web browser: In a secure Web session, the Web browser generates a random encryption key and sends it to the Web site host to be matched with its public encryption key. The browser and the Web site then encrypt and decrypt all transmissions

7.11.2. Digital signatures/certificates: Whereever possible digital signatures are recommended for transmission of sensitive documents over the network via e-mail of other means. By requiring an authentication agent or digital certificate, you force the person on the other end of the transmission to prove his or her identity. In the digital world, trusted third parties can serve as certificate authorities--entities that verify who a user is for you.

7.11.3. Secure FTP: The USOE has established a secure FTP site where authentication is required and all transmissions to and from the site are encrypted. All data files with private or otherwise sensitive information coming into or leaving the USOE network must make use of this site.

7.12. Virus Protection

7.12.1. Antivirus software: All devices, clients and servers attached to the USOE network must have the agency's prescribed antivirus software installed.

7.12.2. Installation: All machines come to the user with the antivirus software agent pre-installed by network staff.

7.12.3. Upgrade/Updates: All updates/upgrades to either the antivirus engine or data files (used to identify virus signatures) are automatically pushed to the individual client machines at logon.

7.12.4. Monitoring: All clients are monitored for currency of their antivirus software. Sometimes machines are so infrequently attached to the network or the automatic updating is unsuccessful that manual intervention is required.

7.12.5. Communication with vendor: Although the latest data/ID "patches" are automatically pushed to the USOE by the vendor, the USOE network staff also monitors vendor initiated and other virus alerts.

7.12.6. Response to attacks: In the case of an actual virus attack a response plan has been established. (see APPENDIX J).

7.13. Backups – USOE Computer Services has long had in place a comprehensive back up system.

7.13.1. Hardware Scope: All servers are backed up including critical operating software for various switches, routers and firewalls. Individual client workstations are not backed up and users are so advised to keep any important data on network servers.

7.13.2. Software scope: All original operating system software, along with service packs and other upgrades, are securely backed up and kept offsite.

Also all commercially purchase and custom developed software are also backed up and kept offsite. This includes all application software.

7.13.3. Backup hardware and software: USOE uses the latest versions of nationally known and highly rated backup software and the models of popular backup drives. Service and support contracts are in place for all backup software and hardware.

7.13.4. Data scope: All user "H:" drives and group "G:" drive are backed up. Also, all database software, documents, web pages etc. are backed-up on all servers.

7.13.5. Backup schedule: (see APPENDIX K)

7.13.6. Encryption: Backup software includes an encryption option when backing up sensitive information to ensure that unauthorized users cannot access backup files.

7.13.7. Verification: USOE's backup software allows for verification of backups to ensure they are written to the disk or tape accurately:

7.13.8. Rotation of backup tapes: New tapes are routinely cycled into the tape library and ones that have gone through too many backup cycles are replaced.

7.13.9. Logs: Logs of all backup dates, locations, and responsible personnel are kept on a daily basis. They are very important if and when data of any type needs to be retrieved form offsite storage.

7.13.10. Test of backup system: Periodically the backup system gets tested when users ask to retrieve some data that was accidentally deleted. Restorations of full servers should also be tested.

7.13.11. Off-site location for critical backup copies: Backups of any and all software, databases, and information that serve critical functions reside in a very secure off-site location and are readily accessible when and if needed. Backup data is treated with the same level of confidentiality as production copies. Periodically checks are made to make sure the backups function as expected.

7.13.12. Off-site frequency: Tape are transported to offsite storage and are picked up on a weekly basis.

7.14. Disaster Recovery/Contingency plans: In 2002 the USOE, in general, developed its first comprehensive contingency and disaster recovery plan. Information Technology was a big part of that plan. The plan is now reviewed and updated twice a year in December and June. The contents of the plan are burned to multiple CD ROMs and distributed to key agency personnel including an associate superintendent, the IT director and the network administrator. Among other items it contains: all emergency contact numbers, hardware inventories; network diagrams; descriptions of how and where all software and data are backed up; formatted descriptions of all USOE systems; circuit lists; and a plan for rebuilding the data center from scratch – (see APPENDIX L)

7.15. Inventories: Inventories of all assets are maintained, including information (data), software, hardware, documentation and supplies. For each server, client workstation and networking device there is included item by item: the manufacturer's name, model, serial number, and other supporting information like operating system, date of install and responsible party.

7.16. Cold or off-site facility: Although a "cold" site that includes everything necessary for resuming operations is not sitting ready and stocked with all the necessary equipment to get up and running after a disaster; the disaster recovery/contingency plan does include some recommended possible sites. Such sites, of course, must have the necessary access and services such as power and telecommunications. After assessing the risks to the USOE the disaster recovery/contingency plan committee decided some delay (up to two weeks) was acceptable, and that the expense to rebuild the entire network can be incurred if and when necessary. The committee identified at least two potential cold sites which have been contacted, and the USOE has received permission to use those sites if necessary. This information is kept as part of the disaster recovery/contingency plan (see APPENDIX M).

8. Training.

8.1. Acceptable Use Policies (AUPs) Keep security reminders visible throughout the workplace (e.g., banner pages, posters, FYI memos, and e-mail broadcasts).

8.2. Security training in general:

8.2.1. Training should be tailored to meet the requirements of the security policy and staffing needs.

8.2.2. Many computer users have never been trained to properly use technology. At most, they many have learned only how to use a particular piece of software for a specific application

8.2.3. The majority may have little understanding of security issues, and there is no reason to expect that to change unless the organization does its part to correct the situation.

8.2.4. Staff must be adequately prepared for making security policies a part of the work environment.

8.2.5. Make a serious attempt at getting the word out to staff, but don't be overly serious in its presentation.

8.3. Training schedule: In addition to new employee training sessions, security refresher workshops should also be held.

8.4. Help Desk: The USOE help desk must be continually promoting security by being alert for situations that might compromise the safety of the USOE network and be ready with security advice and recommendations to individuals and groups of individuals.

8.5. Reference materials: Whenever possible develop and distribute reference materials (e.g., checklists, brochures, and summaries).

8.6. Handbook: Keep the USOE HR rules and employee handbook updated with relevant and current security policies, including the following:.

8.6.1. Who approved the policies
8.6.2. Whose authority sustains the policies
8.6.3. Which laws or regulations, if any, are the policies based on.
8.6.4. Who will enforce the policies
8.6.5. How the policies will be enforced.
8.6.6. Whom the policies affect.
8.6.7. What information assets are being protected
8.6.8. What users are actually required to do

8.6.9. How security breaches and violations should be reported

8.7. Notification: Employees will be told in writing:
- 8.7.1. What is and is not acceptable use of equipment.
- 8.7.2. What the penalties for violating regulations will be.
- 8.7.3. That their activities may be monitored.
- 8.7.4. That agency computers are not for personal use and must not be misused
- 8.7.5. There should be no expectation of privacy for information stored on or transmitted with the organization's equipment.

8.8. Acceptable Use Policy Acknowledgement: Employees are required to sign the agency acceptable use policy that includes security provisions (see APPENDIX I). to acknowledge that they are aware of their responsibilities and verify that they will comply with security policy. This requires that:
- 8.8.1. Staff should have ample opportunity to read and review all policies and regulations for which they will be held accountable.
- 8.8.2. Staff should be provided an appropriate forum for clarifying questions or concerns they may have about the organization's expectations.
- 8.8.3. Staff should not be given access to the system until a signed agreement is accounted for and maintained in a safe place.
- 8.8.4. All new employees should be expected to meet the organization's security requirements and procedures as a part of their job description. Once hired, new employees should be informed of, and trained on, acceptable use and security policies as a part of their initial orientation in order to impress the importance of security upon them.

8.9. Security Training Outline
- 8.9.1. Raise staff awareness of information technology security issues in general.
- 8.9.2. Include broad overview
  - 8.9.2.1. What is information security?
  - 8.9.2.2. Why does it matter?
- 8.9.3. Ensure that staff are aware of local, state, and federal laws and regulations governing confidentiality and security
- 8.9.4. Stress Federal laws
  - 8.9.4.1. FERPA overview
  - 8.9.4.2. FERPA relevance and application (include specific examples that relate to audience duties)
- 8.9.5. Stress state laws, regulations, and standards including GRAMA (Government Records Access and Management Act)
- 8.9.6. Explain organizational security policies and procedures.
- 8.9.7. Ensure that all employees understand that security is a team effort and that each person has an important role to play in meeting security goals and objectives.
- 8.9.8. Train staff to meet the specific security responsibilities of their positions.
- 8.9.9. Inform staff that security activities will be monitored.
- 8.9.10. Remind staff that breaches in security carry consequences.
- 8.9.11. Assure staff that reporting potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making).

8.9.12. Stress that unintentionally destructive acts (e.g., accidental downloading of computer viruses, programming errors, and unwise use of magnetic materials in the office) are the source of many security risks.
    8.9.12.1.
8.9.13. Review results of risk assessment findings along three broad areas that include: assets, threats and vulnerabilities
8.9.14. Review USOE security policies, procedures, and regulations within the main areas and focus on those related to audience's duties.
    8.9.14.1. Physical security regulations
    8.9.14.2. Information security regulations
    8.9.14.3. Software security regulations
    8.9.14.4. User access security regulations
    8.9.14.5. Network security regulations

APPENDIX A

PRIVACY AND USOE DATA

FERPA

1. ***Purpose:*** The federal Family Education Rights and Privacy Act assures parents access to their students' education records and protects the parents' and students' right to privacy by limiting the availability of student records without parental consent.

2. ***Rights established by FERPA:*** There are three general rights: (1) the right to inspect and review education records relating to the student and maintained by the school the child attends or has attended; (2) the right to challenge and require the school to amend a record concerning the student that is inaccurate, misleading or otherwise in violation of the student's privacy rights; (3) the right to require the school to obtain written consent prior to the disclosure of personally identifiable information, subject to specific exceptions.

3. ***"Education records":*** Usually defined as "…those records, files, documents, and other materials which . . . contain information directly related to a student; and . . .are maintained by an educational agency or institution …" regardless of the format the record is in. The definition includes personally identifiable information about students collected and maintained by USOE. This would include student test answers, it does not include the actual tests.

4. ***Parental Consent NOT required:*** USOE does not need to have parental consent to provide data:
   a. ***That is not personally identifiable—***aggregate test scores, for example.
   b. ***To school officials, including teachers, who USOE determines have a legitimate educational interest in the student.*** This might include disclosing the information to the student's teacher, but might not include disclosing it to someone the teacher says should see it.
   c. ***To officials of another school, school system or postsecondary institution where the student seeks or intends to enroll.***
   d. ***To the comptroller general of the United States or the Secretary of Education of state and local educational authorities*** *in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement of or in compliance with requirements related to those programs.*
   e. ***To an organization conducting studies on behalf of USOE*** *to (A) develop, administer or evaluate predictive tests; (B) administer student aid programs; or (C) improve instruction.*
   f. ***To accrediting organizations*** *to carry out their accrediting functions.*
   g. ***To the parents of the student,*** *custodial or non-custodial.*
   h. ***To comply with a judicial order or subpoena****, though the agency must make a reasonable effort to notify the parents about the subpoena before complying with it.*

i. ***In connection with a health or safety emergency***.

5. ***When disclosures are made:***
   a. USOE must create a log whenever it provides personally identifiable information to someone other than the parents. The log should include: (1) the parties who have requested or received the education records; and (2) the legitimate interest the parties had in requesting and obtaining the records. The log should also include the date the request was received and the date records were actually provided.
   b. USOE may charge for the reasonable costs of producing records and need not provide the records in any particular format.
   c. If a parent requests a record, USOE has 45 days to make the record available. FERPA gives parents the right to "inspect" the record, which does not include having copies sent to them. The only time FERPA requires copies is if refusing to copy the record would effectively deny the parent access to the record, i.e. if the parent lives in another state.

6. ***What records does USOE maintain that would be subject to FERPA?***
   d. Test scores attributable to an identifiable individual. Parents have a right under FERPA to see the results of their student's tests. Parents **do not** have a right to see the actual state tests.
   e. Aggregate data that identifies the student because the numbers are so small. For example, an aggregate of the ethnic students who dropout of a particular school or even a district may include so few Asian students that the students become identifiable because there are only two Asian students in the district. Data that does identify students in this matter must be used in compliance with FERPA.
   f. Student enrollment data. USOE is **not** a general source of information regarding the location of students. Persons seeking to know where a student is enrolled must be the parent of the student and/or have court documentation requiring USOE to release the data, per FERPA.

GRAMA—Government Records Access and Management Act

1. Teacher records: CACTUS records are not protected by FERPA. Anyone can request access to CACTUS data, but GRAMA only requires USOE to provide certain specified information about employees: work phone numbers and addresses, gross compensation, job descriptions and the teacher's qualifications for the job, such as college degrees earned.
2. USOE must respond to a GRAMA request within 10 days of receiving it. The response may be "no, and here's why (the information doesn't exist, you aren't entitled to receive it, etc)," "Yes, and here you go," "yes to the attached items and no to the rest of your request," or "yes, but we need x number of days or weeks to compile the data." GRAMA requests for anything other than data that is clearly public record should be forwarded to USOE Legal for review.

APPENDIX B

USOE Power Users Guide
03-11-2004

Definitions:

Standard User: Most USOE users, about ninety percent, fall into this category. These users have full access to USOE services and, where appropriate, they have permission to write to certain directories on certain servers. The services include among others: e-mail, customer applications, Internet browsing, desktop productivity tools (word processing, spreadsheets etc.), as well as the ability to store data on local storage devices and sync handheld devices. What a standard user cannot do is alter the basic configuration of or install software on agency computers. As with the other user definitions given here, this a general one. Actual definitions can to customized according to multiple sets of rights (e.g changing the system time, installing DLLs) and permissions (e.g. read only, write).

Administrative User: This user generally has complete access to all the USOE technology resources. There should probably no more than a handful of administrative users in the organization. Such users can install and configure servers as well as desktop machines. They can control the access and permissions other types of users have to technology resources.

Power User: A power user is closer to a standard user in capabilities than to the administrative user, having a similar range of rights and permissions. The power user has more control of the local machine than the standard user. While the standard user can save data on the local machine and change certain properties such as desktop themes, the power user can install software after receiving permission from the network administration staff. The software the power user can install may include new versions or enhancements to the basic operating system or other system software such as PDA synchronization devices. In the case of a power user who is also a USOE Zone Administrator, they will also be able to perform those same services for standard users within their zone.

Qualifying to be a Power User:

- Network Professionals: By definition, administrative users, who are almost always professional network specialists and are very limited in number, are also power users.

- Zone Administrators and Automated System Support Specialists: By nature of their special assignments, in sections where such individuals have been designated, they are power uses. In some cases, due to the duties specific to their assignments they may have even more rights and permissions than the typical power user. Examples include someone who needs to grant security permissions to users on a server or install software on other users' mahines.

- Developers/Programmers/Web Masters: Anyone who develops custom software may have a need to have greater access to their local machine resources than a standard user. Such positions frequently require the installation and removal of various types of software that include but are not limited: to software development software, database systems, and software management tools.

- Other users who may qualify as power users: Although requests for the status of power user will ultimately have to be considered on a case-by-case basis by the professional network staff and, require the sign-off of the requesting user's supervisor; the following is a representative list of those who may qualify. Ultimately, qualification depends on the scope and frequency of activities such as those described herein.

    - Curriculum specialists who frequently need to evaluate various computer based instructional packages from commercial and other sources

    - Media specialists who often need to install software used in the production of media or various computer based instructional packages from commercial and other sources

    - Statisticians who frequently need to install and/or upgrade software required to do various types of statistical analyses

    - Others who can demonstrate power user needs similar to those described herein.

Procedures:

- The prospective power user can be identified either by himself or herself, a supervisor, or the network staff.

- The prospective power user is required to submit a written request to the USOE IT Manager explaining power user status should be granted. This request must be signed by his or her supervisor or forwarded via e-mail from his or her supervisor.

- The IT Manager along with network administration staff will review this request and notify the applicant and supervisor whether or not they agree with the request. If the requst is agreed upon the applicant will be granted appropriate rights and permissions.

- While functioning as a power user, the user is still required to follow the agency's and state's acceptable use policy.

- The power user must always notify network staff what software they are planning to install before doing so. Network staff will review and respond to these requests as top priority items. Special arrangements may have to made in some cases to cover emergency situations.

- The power user must be especially vigilant to ensure against installing any unlicensed software.

- In the event the power user has technical problems with his or her machine as a result of some installation or modification they perform, and need assistance, they will need to submit the usual help desk request. Their status as power users does not imply priority service from the network staff.

- If the power user encounters repeated problems requiring network staff intervention, they may be referred to additional training or have the power user status revoked.

APPENDIX C

DATABASE SOFTWARE				
Access 2.0	MS	x	x	
Access 7.0	MS	x	x	
Works for Mac	MS	x	x	
PRESENTATION SOFTWARE				
PowerPoint (Win 3.1)	MS	x	x	
PowerPoint (Win 95)	MS	x	x	
PowerPoint for Mac	MS	x	x	
WordPerfect Presentation (Win 3.1)	Corel	x	x	
WordPerfect Presentation (Win 95)	Corel	x	x	
Astound	Gold…			
OTHER DESKTOP SOFTWARE				
Calendar Creator Plus				
WinZip 3.x				
WinZip 95				
PK Zip Utilities				
Windows 95 Plus	MS	?	?	
Informs	Novell	x	x	
Slide Sshow Screen Saver				
PageMaker for Mac	Aldus			
PageMaker for Windows	Aldus			
Microsoft Project (Windows)	MS	x	x	
Norton Utilities for Windows	Symantic			
Norton Utilities for Mac	Symantic			
PageMill HTML Editor				
FrontPage HTML Editor	MS	x	x	
SAM Anti Virus for Mac				
PowerBuilder (Enterprise Developer)	PowerSoft	x	x	x
Harvard Graphics	SPC	x		
LAN Workplace (Win)	Novell	x	x	
Desktop DBA	Datura			
Net FAX				
SQA Team Test				
Natural Connection	Software AG	x		
ECS (Job Scheduler)		x		
Realia Cobol	CA	x		
Robo Help	Blue Sky			
Erwin	Logic Works			
Falcon	Phoenix	x	x	
SNA				
FiNet				
Rumba	Wall Data	x		
Visual Basic	Microsoft	x	x	
DSDesigner (FiNet)				
Sybase Sql Anywhere	Sybase	x		
SPSS for Windows				
Quattro Pro V.7	Corel			
Nutri Kids				
Disney Interactive				
MS Frontpage	MS			
MS Publisher	MS			
MS Works (Windows)	MS			
PrintShop Deluxe				

USOE (Agency) CUSTOM SYSTEMS

Division	Name	Purpose	Hardware	Network
Agency Support	CACTUS	Statewide tracking of certificated educators	Intel	UEN
Agency Support	AFR	Annual Financial Report from school districts	Intel	UEN
Agency Support	S3	Annual Student Statistical Reports (Year End, Fall, Class Size, Adult Ed etc.)	Intel	UEN
Rehabilitation	IRIS	Integrated Rehabilitation Information System (clients & payments)	Intel	ITS
Agency Support	Minimum School	Disbursement of funds to school districts, detailed revenue & recipient accounting	IBM Mainframe	ITS
Agency Support	Transportation	Collection and accounting of school busing data	Intel	UEN
Agency Support	Network Inventory	Local LAN resource control	Intel	Local LAN only
Agency Support	Warehouse	State and Federal Reporting	Intel	UEN
Instructional Services	AIMS	Approved and pending Instructional materials database	Intel	UEN

USOE (District) CUSTOM SYSTEMS

Name	Purpose	Software	Database	External Interfaces
Student InformationSystem Mainframe	Student Service Applications	Cobol MVS	Adabas/VSAM	School Districts
SchoolNet	Student Service Applications	Visual Foxpro	SQL Server	School Districts
Fiscal Systems Mainframe	Financial Services	Cobol MVS	ADABAS VSAM	School Districts
Fiscal Systems Micros	Financial Services	Foxpro 2.6	Foxpro	School Districts
Testing Systems	Scanning and Scoring of statewide CRT and SAT tests	Cobol MVS Visual Foxpro	Adabas VSAM	
Clearinghouse	Collection and distribution of ACCT & Student DATA	Foxpro Cobol MVS	Sybase 1.1x	
District Billing	Billing Statements to Districts for Services	Cobol MVS	VSAM	

APPENDIX D

USOE SOFTWARE LICENSES

Company	Product
Adobe	Acrobat 5.0
Adobe	Fireworks 4.0
Adobe	Paintshop Pro 6
Adobe	Photoshop 6.0
Adobe	Photoshop 7.0
Adobe	Pagemaker 6.5
Bluesky	Robohelp
Boreland	Jbuilder
Cisco	Advantage Firewall PIX 525 Maintenance
Computer Asso	ERWin
Computer Asso	Desktop DBA
Corel	Office Suite Standard Edition
Corel	WordPerfect 6
Embarcadero	DBArtisan
eEye Digital Sec	Retina Professional Edition-32 IP Pack 4.0 Windows
Harvard	Harvard Graphics - Obsolete?
IDM Computer S	UltraEdit-32
InstallShield	InstallShield 5.5
LinkPro	Powersync Server
Lotus	ScreenCam NU WIN/NT 5.0
MacroMedia	Dreamweaver 4.0
MacroMedia	UltraDev 4.0
McAfee	Active Virus Defense Suite
Microsoft	Exchange CAL 2000
Microsoft	Windows CAL 2000
Microsoft	Project 4.1
Microsoft	Publisher 97
Microsoft	Visual Basic 5
Microsoft	Frontpage 97
Microsoft	Frontpage 2000
Microsoft	Exchange ACD Exch Conn V5.0 B
Microsoft	Exchange ACD Exch Intnet Mail B
Microsoft	Exchange ACD Exch Srv Ent v5.0 B
Microsoft	Exchange ACD Win NT Srvr v4.0 Lev
Microsoft	Multiview Viewer Royalties for 105 copies
Microsoft	Office Professional 2000
Microsoft	Office Professional XP
Microsoft	Windows 98 Upgrade
Microsoft	Windows XP
Microsoft	Windows 2000 Professional
Microsoft	Windows Terminal Services CAL
Microsoft	Windows Terminal Services Internet Connector 2000
Microsoft	Powerpoint 2000
Microsoft	Paintshop Pro 7
Microsoft	Windows Advanced Server 2000
Microsoft	Windows Server Enterprise 2003
Microsoft	Windows NT Server 4.0
Microsoft	SQL Svr 2000
Microsoft	Visio Pro 2002
Nemx	Nemx Anti Virus MXS-R
Netopia	Timbuktu Pro 32
Network Associ	Sniffer Basic 3.5
Phoenix	Falcon 5 User, Networked
Powerquest	DriveImage Pro
PowerQuest	Partition Magic

APPENDIX E

Software Development Life Cycles: Outline for Developing a Traceability Matrix

By Diana Baldwin, AccuReg Inc.

1. Software Life Cycle
    1. The FDA does not prescribe a specific software development life cycle, but requires manufacturers to identify and follow what makes sense for them
    2. Manufacturers choose a software life cycle model and development methodology appropriate for their device and organization
        1. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 1998
    3. Software Life Cycle must include:
        1. Risk management
        2. Requirements analysis and specification
        3. Design (both top level and detailed)
        4. Implementation (coding)
        5. Integration
        6. Validation
        7. Maintenance
    4. A software life cycle model should be understandable, thoroughly documented, results oriented, auditable, and traceable.
        1. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 1998

2. What is required to demonstrate traceability?
    1. Provide a traceability analysis or matrix which links requirements, design specifications, hazards, and validation. Traceability among these activities and documents is essential. This document acts as a map, providing the links necessary for determining where information is located.
        1. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 1998

3. How Does Traceability Ensure the Life Cycle is Followed?
    1. It demonstrates the relationship between design inputs and design outputs
    2. It ensures that design is based on predecessor, established requirements
    3. It helps ensure that design specifications are appropriately verified, that functional requirements are appropriately validated
    4. Important: Traceability is a 2-way street. Maintain "backwards" and "forwards" -- Tunnel Vision not acceptable in the Software Life Cycle!

4. Traceability Across the Life Cycle
    1. Risk Analysis (Initial and Ongoing Activities)
        1. Trace potential hazards to their specific cause
        2. Trace identified mitigations to the potential hazards
        3. Trace specific causes of software-related hazards to their location in the software
    2. Requirements Analysis and Specification
        1. Trace Software Requirements to System Requirements
        2. Trace Software Requirements to hardware, user, operator and software interface requirements
        3. Trace Software Requirements to Risk Analysis mitigations
    3. Design Analysis and Specification

1. Trace High-Level Design Specifications to Software Requirements
2. Trace Design Interfaces to hardware, user, operator and software interface requirements
3. Evaluate design for introduction of hazards; trace to Hazard Analysis as appropriate

4. Design Analysis and Specification
    1. Trace Detailed Design Specifications to High-Level Design
    2. IMPORTANT: Ability to demonstrate traceability of safety critical software functions and safety critical software controls to the detailed design specifications
5. Source Code Analysis (Implementation)
    1. Trace Source Code to Detailed Design Specifications
    2. Trace unit tests to Source Code and to Design Specifications
        1. Verify an appropriate relationship between the Source Code and Design Specifications being challenged
6. Source Code Analysis (Implementation)
    1. Trace Source Code to Design Specifications
    2. Trace unit tests to Source Code and to Design Specifications
        1. Verify an appropriate relationship between the Source Code and Design Specifications being challenged
7. Integration
    1. Trace integration tests to High-Level Design Specifications
    2. IMPORTANT: Use High-Level Design Specifications to establish a rational approach to integration, to determine regression testing when changes are made
8. Validation
    1. Trace system tests to Software Requirement Specifications
    2. Use a variety of test types
        1. Design test cases to address concerns such as robustness, stress, security, recovery, usability, etc.
    3. Use traceability to assure that the necessary level of coverage is achieved

5. Plan Ahead for Traceability
    1. Options
        1. Manual methods
            1. Word processors
            2. Spreadsheets
        2. "Home-built" Automated Systems
            1. Relational Databases
        3. Commercial Automated Systems
            1. DOORS
            2. Requisite Pro

APPENDIX F

USOE CHANGE REQUEST FORM FOR COMPUTER SERVICES (CR-1 Aug 2004)

Section 1: Change Request Information

To be completed by Requester except shaded areas, see DETAILED INSTRUCTIONS BELOW

All requests should be e-mailed by an Associate Superintendent to dwhite@usoe.k12.ut.us

Originator (Title)		**CR Type:**	☐ **Change to Existing System or Project** ☐ **New System or project** ☐ **Other Temporary or One-Time Project**
Director/Coordinator			
System Name			
Or… Project Name		**CR No:**	
Or… Other		**CR Log Date:**	
		CR Resolved Date:	
Desired Date			

1A – Description of Change Being Requested: (Describe the requested change. Provide attachments if additional explanation is needed.)

1B - Proposed Solution: (Provide your opinion regarding the best course of action, based on factors such as cost, schedule, or product quality. Provide attachments if additional explanation is needed.)

1C - Risk Impact: (Provide your opinion regarding the risk of not doing the change, based on factors such as cost, schedule, or product quality. Provide attachments if additional explanation is needed

1D – Quality Assurance/Controls: (Describe how you plan to help provide for quality of the data/information involved in the system/project. What controls will be implemented and who will be responsible to work with Computer Services to ensure

USOE CHANGE REQUEST FORM FOR COMPUTER SERVICES (CR-1 Aug 2004)

such quality and controls. Provide attachments if additional explanation is needed.)

Section 2: Priority Assessment (Use Service Level Agreements in Change Management Process Document)

Service Level Agreement Used: ☐ **Applications** ☐ **Project** ☐ **Other**

Assigned Service Level: ☐ **(1)** ☐ **(2)** ☐ **(3)** ☐ **(4)** ☐ **(5)** ☐ **New Project Required**

2A – Justification for Priority

Section 3: Impact Analysis (To be completed by Computer Services or Project Management)

3A - List Artifacts Affected

5B- Overall Impact:

Business Assessment: (Briefly describe the anticipated benefits, and document any changes to the workflow/operational procedures which might result from this change.)

Completed by: *Date:*

Technical Assessment: (Briefly describe how existing services or deliverables will be affected as a result of the requested change. Describe acceptance criteria for changed deliverables. Attach documentation such as the functional

USOE CHANGE REQUEST FORM FOR COMPUTER SERVICES (CR-1 Aug 2004)

specification to illustrate, as needed.)

Completed by: *Date:*

Cost Assessment: (Briefly describe changes to the Resource Plan that would result from this change.

Time Assessment: (Briefly describe changes to the Project Schedule that would result from this change. Attach copies of existing and new schedules showing new tasks, subtasks, and milestones.)

Completed by: *Date:*

3C- Potential Risks:

3D – Management Approval:	**Phone:**	**Date:**

Section 4: Disposition of CCB (To be completed by Computer Services or Project Management)

Disposition Assigned:	☐ Pre-Approved	☐ Approve	☐ Deny	☐ Defer	☐ More Info

Assigned Service Level:	☐ **1 (Pre-Approved)**	☐ **2**	☐ **3**	☐ **4**	☐ **5**	☐ **New Project Required**

Changes which are not approved within ten (10) work days will be considered to be rejected.

4A – Recommendations and Communication Plan/:

4B – Action Items

Action Item	Due Date	Responsible	Status

4C - CCB Approval: (Project Management Office)	**CCB Date:**

Section 5 - Closure	**Completed**	**Date Completed**
· Communication to impacted parties	☐	
· Artifacts updated	☐	
· Project Plan updated	☐	

Instructions

- Orignator fills in Section 1 *(excluding the CR number assignment, Logged Date and Resolved Date)*
  - *Specify if CR is for an existing system (including IT infrastructure) OR existing project OR other*
  - *If CR is for an existing system or project, specify the parts of the system/application needing change. Provide details in section 1. See examples below.*
  - *If CR is for a project, specify the deliverable where the change would occur.*
- PMO assigns the next available Change Request Number
- Project Management completes Section 2
- CCB completes Section 3
- Project Management completes Section 4

Section 1 (General information)	
· Provide unique description · Enter Priority Rating · Enter date needed by	***Examples: Forms, Reports, Data Field, Labels, Color, Business Rules, Error messages, Desired services, Desktop environment, etc.***
Section 1A (Requester's Description of Change) · Explain why the change is required · Provide a narrative of any problem	***Provide business or technical justification. Provide a step by step description of any problem so that it can be reproduced by the computer services staff.***
Section 1B (Proposed Solution) · Provide a brief description of proposed solution	
Section 1C (Risk Impact) · Provide a brief description of risk if change is not made	**Describe the consequence of not implementing the CR. Describe consequences of implementing the CR**
Section 2A (Impact Analysis)	**Identify who performed the assessment in each sub-section.**
· List Artifacts affected and their owners	**List all artifacts requiring work if the change is implemented. Use *Impact Analysis For.* Place summary of impact in this section. List all new, modified or deleted artifacts**
Section 2B (Overall Impact) · Explain how each artifact or function is affected · List all processes and functions affected	**Describe the following criteria:** · **Work: Expected number of hours to complete the change** · **Resources: The types of resources needed and their availability. Describe conflicts with other work assignments** · **Schedule: Estimate the amount of time in calendar weeks to implement the change. For projects, calendar days should be used.** ·
Section 2C (Potential Risk) · Identify potential risk(s) · Obtain Project Manager's approval	
Section 2D (Track Lead Approval)	

- Director of Computer Services must approve all CR's in order to be submitted to CCB for disposition

Section 3 (Priority Assessment)

- Service Level Agreement Used
- Priority Assigned
- Justification for Priority

Section 3 (Disposition of CCB)

- Status
- Recommendation
- Action Items
- CCB Approval

Section 4 (Closure)

- Notify affected entities
- Artifacts updated
- Project Plan updated

APPENDIX G

ACS Custom Software Applications Requests

Definitions

- The application **owner** is the business or organizational unit responsible for the data and business processes the application is designed to facilitate through automation. Examples include the Educator Licensing, Internal Accounting and School Finance sections.

- **Request books** (Excel workbooks), one for each development team, are stored in the following directories: //begroups/acs$/requests/team_name.xls where **team_name** can be: cactus-iris, financial, or warehouse. Individual, detail **request documents** are stored in the same directories and follow the naming convention: **team_name** + **developer**_initials + date + alpha_character. The date should be in the format of yymmdd. The alpha character should be "a", "b" etc. and only used to distinguish two or more request documents created by the same **developer** on the same day.

- The application **liaison** is the person who provides the primary means of communication between the **owner** of the application and the application development team, specifically the team **leader**. As problems or issues with the application arise the liaison does the initial screening to determine which problems or issues need to be defined as **requests** for the development team. Such raw requests should initially flow from the **liaison** to the team **leader**.

  Later in the request process additional individuals from both the **owner** community (also called **customers**) and the development team may need to become involved. Regularly scheduled project or application meetings in which both **customers** and **developers** are present may also serve as a place for the initial definition of a request.

- The development team **leader** is the person responsible for defining the request in the request book after communications with the application **liaison**. The **leader** also assigns and monitors the progress of the request. More details follow in the **Status and Procedures** section.

- The application **developer** (programmer or database analyst classsification) is ultimately responsible for the completion of the request. Often the team leader will also assume the role of the application **developer**. See status descriptions below for more details on how the developed and team leader move the request through the various steps to completion.

- IT **management** is the individual(s) responsible for the general delivery of information technology to the Utah State Office of Education, and specifically in the the form of custom software applications.

Status and Procedures

Unassigned

The team **leader** makes an initial evaluation of the request received from the application **liaison.** If more clarification is necessary the **leader** will communicate with the **liaison** or other **customers** to gain more understanding of the request and establish a **priority**. The three **priority** levels are: **1** (high), **2** (normal), and **3** (low). Throughout the course of the request only the **leader** should modify the request's **priority**.

At this point the team **leader** creates a row for the request in the appropriate **request book**. All columns must be completed except the **assigned-to** column, unless the status is going to immediately be changed to **assigned**. The request **description** should be kept reasonably brief. The **request document** linked to from the **request document** column should contain the detailed problem, design, and testing information.

Assigned

When the team **leader** decides which application **developer** is to be assigned to the request, the **assigned-to** column is filled-in and the status is changed to **assigned**. When this change of status occurs a message will be emailed to the **liaison**, the **developer**, and any designated **management**. All messages triggered by status changes will include: the **description** of the request, the **liaison**, the **request date**, the **due date** (if specified) and the **developer** to whom the request was assigned.

In-progress

The **developer** to whom the request is assigned changes its status to i**n-progress** when he actually begins work on the request. This is done only after he has completed the **request document** and have inserted a link pointing to that document. The naming convention for the **request document** is described in the **request books** paragraph at the top of this page. Changing the status to **in-progress** will trigger a message to the **leader** and the **liaison**.

If, for whatever reason, progress towards the completion of the request is stopped (usually for a week or more) the status of the request may be moved back to just **assigned** or even **unassigned**. Only the **team leader** should make such a change.

Completed

After the new or changed features of the request have been fully tested by the **developer** he will change the status of the request to **completed**. When this

change of status occurs a message will be sent to the **liaison** originating the request and the **leader**. This should only be done after the **developer** has reviewed their work against the **request document**. In some cases a code walk-through with another **developer(s)** may be desirable.

Production

After the **leader** agrees the request has been satisfactorily completed he will move the request to **production** status; but only after the necessary components that were added or modified have been physically moved to the **production code directory** and any **production database** changes have been made.

Sometimes the **leader** may instruct the **liaison** or their designees to do some "beta" testing with test data before this is done. If, for whatever reason, the **leader** thinks more work needs to be done he may move the request back into **active** status after discussing the problem with the **developer**.

The exact process of moving the new code into **production** will vary depending on the architecture. Here us an example in which Powerbuilder is the architecture and BASE is the application.

- All source code libraries (.PBLs) are moved from //begroups/acs$/pb/base to //beusoe2/acsapplibs$/base/source.
- The source code in //beusoe2/acsapplibs$/base/source is compiled into .PBDs and .EXEs in //beusoe2/acsapplibs$/base/object.
- These new PBDs and .EXEs are copied into the appropriate directories on servers for: launching by users, synchronization by standalone installations or packaging into Installshield zip files. In the case of CACTUS these directories would respectively be: //beusoe1/winapps/cactus, //beweb/pub/acs/cactus/sync and //begroups/acs$/install/55/cactus/pbds.

APPENDIX H

USOE Network Standards and Connection Policy

(Definitions of *bold & italicized* terms are listed at the bottom.)

Three classes of computers may connect to the *USOE network*. Please note the restrictions that apply to each class.

1. **Owned by the USOE.**

   This computer may be connected directly to the ***USOE domain*** via cable.

   All USOE owned machines are purchased, installed, configured, and maintained according to ***USOE hardware and software standards*** by network administrators.

   Additional software may be installed only with the approval of the USOE network administrators. If the USOE owned computer is a notebook, it may also be used for ***telecommuting.*** It may be configured for ***VPN*** to access the ***USOE domain*** from the Internet or through the ***USOE wireless network segment***.

2. **Employee owned and approved for *telecommuting*.**

   The employee must assure the USOE in writing the employee owned computer meets requirements for ***telecommuting***. This includes meeting USOE ***secure computer*** requirements. ***VPN*** can be used to connect to the ***USOE domain*** over the Internet, usually from home. USOE network administrators may not directly assist in the installation, configuration, or maintenance of an employee owned computer.

   A USOE employee who has had an employee owned notebook computer approved for ***telecommuting,*** may bring that device on site. However, it may only be connected to the ***USOE domain*** through the ***USOE wireless network segment*** in conjunction with ***VPN***.

   Only USOE owned computers and employee owned computers approved for *telecommuting* may be connected to the *USOE wireless network segment* and to the *USOE domain* through *VPN* or any other means.

   No other employee-owned devices are permissible and all connections must be made in the above manner. Machines in violation of this policy will be disconnected from the network, and the user will be denied further access until USOE network administration has discussed the violation with the violator's supervisor. **Violators may be subject to disciplinary action**. Prohibited devices include all peripherals (e.g. printers and scanners). See note about PDAs below.

3. **Privately owned and brought into the USOE by a business visitor.**

   A business visitor may access the Internet, but not the ***USOE domain***. To access the Internet they must receive permission along with current codes from a USOE sponsor/host in order to connect to the ***USOE wireless network segment***. With

these codes the business visitor is responsible for configuring, and establishing only a wireless Internet connection. If the business visitor does not have a wireless network adapter, they may still connect to the Internet via cable and specially marked data jacks in conference rooms throughout the building.

The business visitor must be asked to assure their host they are using a ***secure computer*** and are willing to abide by the ***Acceptable Use Policy***.

Note about PDAs (personal digital assistants). No PDA or other handheld device may, by itself, be directly connected to the USOE network, wirelessly or with cable. When properly configured such devices may be used to synchronize with the host computer or download network files including those in Outlook, This is only permissible through a USOE owned or ***telecommuting*** computer by means of an attached cradle or Bluetooth wireless technology. **Violators of this policy may be subject to disciplinary action.**

USOE is not responsible for lost data or damage to any privately owned machine that is connected to *USOE wireless network segment* or the *USOE domain*.

Definitions

Acceptable Use Policy. All employees and business visitors, regardless of how they are connected to the USOE network are required to follow the USOE acceptable use policy. See: http://www.usoe.k12.ut.us/hrm/acceptuse.htm & http://www.governor.utah.gov/lan/aup.htm.
Also note the acceptable use policy states:

Also, please note the acceptable use policy states that the use of resources for personal reasons on a more than incidental basis or for mass distribution of chain letters, jokes, etc., or other uses that waste resources or disrupts performance, is prohibited.

This includes use of agency machines for streaming audio and video when not work-related. **Violations of the acceptable use policy may be grounds for termination.**

Secured computer. In order to be secured, a computer must meet the following criteria. It must have the latest up-to-date virus protection software installed and running. The computer must also have strong-password protection and not have any of the following services running at any time it is connected to the USOE network: peer-to-peer networking, file-sharing, instant messaging, or network broadcasts of any kind. McAfee virus protection software is available for home use by any USOE employee. Please see a network administrator for a copy.

Telecommuting. USOE employees may telecommute with management approval. In the application process Computer Services reviews and approves the telecommuter's computer configuration. While the telecommuter is given freedom to choose the employee owned computer's make and model; the machine must still be documented as

being able to perform the tasks required of the telecommuter and be secure, posing no foreseeable threat to the USOE network. If the telecommuter desires to connect to the ***USOE domain*** through the Internet and ***VPN***, they must secure their own Internet connection and configure any employee owned machine to do so. Only general directions for ***VPN*** configuration and virus protection software installation will be available to those using employee owned machines for telecommuting. See http://www.usoe.k12.ut.us/hrm/rules2002.pdf for more information about telecommuting.

USOE domain. The USOE domain is the secure network of shared computers at the USOE. It is a subset of the more generally defined ***USOE network***. The domain includes all servers and user computers, each connected to one or more of those servers. These machines are all behind a firewall and other security devices and software such as intrusion detection and filtering servers. When a user connects to the USOE domain from within the building by supplying a logon name and password they also receive Internet access. Business visitors are permitted to connect to the USOE wiring infrastructure and obtain Internet access without connecting to the USOE domain. Such use is permitted only through the ***USOE wireless network segment***.

USOE hardware and software standards. In order to maximize usability, reliability, security, and efficiency of USOE information technology resources; the USOE has defined hardware and software standards. A summary of the current hardware/software standards include: a Dell or MPC desktop or notebook running Windows XP with Service Pack 1 installed, and the Microsoft Office 2000 suite of productivity applications including the Outlook e-mail/groupware client. As part of the USOE standard setup features, these machines are all configured as ***secured computers***. Other hardware and software standards exist in the USOE, but most involve network infrastructure and custom application development and deployments. Always check with network administrators before purchasing software or hardware to see if it is compatible with the USOE network, and if an agency license agreement (in the case of software) already exists.

USOE network. The USOE network is defined as the entire computer infrastructure within the USOE including all wiring, communication devices, routers, switches, servers, desktops and other connected computers. The ***USOE domain*** is a subset of this network.

USOE wireless network Segment. A secure wireless network segment is available for USOE staff and sponsored business visitors. This network provides access to the Internet and optionally to the USOE domain via VPN. In order to connect to the USOE for Internet and/or USOE domain access, the USOE employee or business visitor must first acquire the current wireless SSID (secure site ID) and WEP (wireless encryption protocol) codes and configure the computer to recognize and connect to the USOE wireless network segment. For security reasons these codes will change periodically. When this happens they will be distributed to all USOE employees who have a VPN account. Currently the USOE supports the IEEE 801.11b and 801.11g wireless protocols.

VPN (virtual private network). VPN allows those with USOE domain accounts to access the USOE network remotely or through the firewall. You must have a VPN account established by a USOE network administrator before you can access the domain using VPN. Only general directions for VPN configuration and virus protection

software installation will be available to those using employee owned machines for ***telecommuting***.

APPENDIX I

Information Technology Resources
Acceptable Use Policy

This statement of policy has been adapted (as of 1/26/98) from Appendices A and B to the State of Utah Information Technology Resources Acceptable Use Policy as adopted by the Information Technology Policy and Strategy Committee on August 15, 1996. It is also consistent with the UEN Public Education Acceptable Use Policy

The USOE/USOR characterizes as unacceptable and just cause for termination of use privileges, disciplinary action, and/or legal action, any of the following uses of information technology resources--e.g., computers, copiers, e-mail, fax, Internet, printed material, printers, video--provided by the agency:

1. Illegal Use. Any use for or in support of activities that violate local, state, or federal laws.

2. Infringement of Intellectual Property Rights. Any use in violation of software license agreements or other contractual arrangements relating to the use of copyrighted information.

3. Commercial Use. Any use for commercial purposes or activities resulting in personal financial gain, including product advertisements.

4. Personal Use. Any use for personal reasons on a more than incidental basis or for mass distribution of chain letters, jokes, etc.

5. Offensive or Harassing Material. Any use of material which may be deemed vulgar, sexually explicit or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, or political or religious beliefs.

6. Religious or Political Lobbying. Any use for religious or political lobbying.

7. Security Violations. Any action which threatens the security of agency resources, including but not limited to such actions as: giving your password to another person; accessing accounts for which you are not authorized; or spreading computer viruses.

8. Confidential Information. Transmitting information classified as other than "public" under the Government Records Access and Management Act without proper security; or violating the privacy of others by reading e-mail or other private communications (unless you are specifically authorized to support communication systems).

9. Unnecessary Use. Otherwise appropriate use which intentionally wastes resources or disrupts performance by excessively consuming operating time, storage, paper, etc.

APPENDIX J

USOE COMPUTER VIRUS RESPONSE PLAN

USOE Anti-virus Environment

E-mail Servers - All incoming e-mail and attachments are scanned and cleaned, if necessary, by the Barracuda SPAM and anti-virus Firewall before going to the e-mail server. Barracuda signature files are updated on a daily basis. If an e-mail message or attachment is found to have a virus it is deleted, logged and replaced with a message notifying the user that this has occurred.

Servers - All servers, including e-mail servers, have the McAfee Virus Scan product installed to check on a daily basis for updated DATS (signature files). It is also checks on a biweekly basis for any upgrades of the anti-virus scanning engine. This product checks all files coming into the server for viruses.

Clients - All client Machines have the McAfee Virus Scan product installed in such a way that it checks on a daily basis for updated DATS (signature files). It is also checks on a biweekly basis for any upgrades of the anti-virus scanning engine. This product checks all files coming into the computer for viruses.

Staffing assignments

Baarracuda Spam Firewall (Jared Southwick/ Dave Hughes)

Coordinator/Mail Server Administrator (Mark Wagstsaff / Jared Southwick)

Client & Server Anti-Virus Software/Data Recovery (Alan Ericksen/ Jared Southwick)

Help Desk/Telecommunication (Carla Worthen / Alan Ericksen)

Virus Outbreak Procedure

Virus attacks are an ongoing occurrence. Every day hundreds or thousands of infected e-mails arrive at the e-mail server. Over 99% of these are successfully intercepted by the Barracuda SPAM Firewall (deleted and logged) and cause no damage. A virus can also be introduced from downloads or file copies from other magnetic media. In these cases, the vast majority are detected and deleted by the McAfee anti-virus software. However, on occasion,

a machine or machines can get infected. The following is a procedure to be followed in these events. Note, that not every instance of an infection warrants network-wide response. Often the problem can be isolated an dealt with on one machine.

- As a regular preemptive step, the Barracuda Firewall administrator should regularly check the log generated by the Barracuda system to determine if the USOE network is being hit by a heavier that normal number of e-mails or virus contained in messages or attachments. Although the log indicates when viruses have be intercepted and "cleaned", either event may be cause to be on the lookout for other incidents.

- As soon as a reported problem (usually via the help desk) on a client machine or desktop looks as if it is a possible virus, the machine should be disconnected from the network, until the machine can be fully scanned by the most current anti-virus software and it can be determined that it is free from any new undocumented virus.

- If a virus is identified, the anti-virus software web sites should be searched to determine the behavior or the new virus. If no virus is found, but an apparent infection has taken place, an attempt should be made to match the symptoms with those of newly reported viruses in an attempt to identify the cause of the infection. Again, the anti-virus software vendor web sites should be employed.

- Once the virus has be researched and identified. The directives from the web sites should be followed to mitigate the impact on the internal and external networks.

- If the virus is high risk or widespread, consideration should be made for either shutting down the e-mail server, disconnecting the internal USOE network from the external (Internet) network or both. This decision should be made by the coordinator and communicated from the help desk by e-mail (if possible) to all users, or by phone if e-mail is not operable. In part, this decision may be made based on the volume of e-mail leaving the e-mail server for internal, or more importantly, external destinations. A rapidly increasing volume of e-mail may indicate the virus is being proliferated by the USOE's e-mail server.

- The decision to disconnect the network may also need to be made if the network or parts of the network are under attack from a hacker of some type. Such attacks will more than likely affect only isolated machines (clients or servers), but the potential exists for having to isolate the entire network.

- After all affected machine or mailboxes have been identified and the virus has been contained and cleaned, there may be the need to recovery corrupted data from backup servers or tapes. If the damage is widespread, ad hoc priorities by have to be defined and communicated concerning whose files and/or mail will be restored first.

- Finally, the incident should be described and logged, with recommendations for future prevention.

APPENDIX K

USOE Back-up/Data File Recovery Procedures

Definitions:

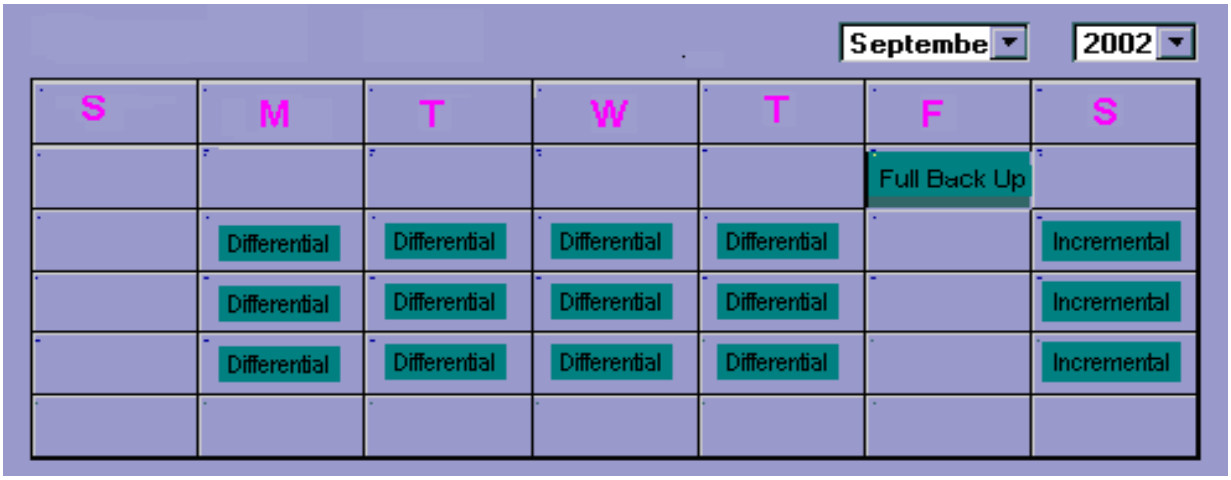
Full	A full backup is a complete back up of files and the archive bit is reset.
Differential	A differential backup **does not** reset the archive bit and will back up all files that have changed since the previous resetting of archive bit.
Incremental	An incremental backup **does** reset the archive bit and will backup all files that have changed since the previous resetting of the archive bit.

A contract with an off-site storage facility, Perpetual Storage Inc., has been executed. Telephone number: (801) 942-1950. (See Attachment A) This facility is a fully finished, multi-mezzanine storage area located in a granite vault. It is a guarded facility to which only Perpetual Storage personnel are allowed. Backups are created, labeled and put in boxes, which are picked up and taken to the storage facility on a regularly scheduled basis. Taped back ups are scheduled to leave the USOE building every Tuesday morning of the year. (USOE staff is responsible to schedule pick up times during holidays.)

The process is as follows: (Figure 1, Tape Backup Schedule)

- A full back up is run the first weekend prior to the first Tuesday of the month.
- On the first Tuesday of each month, the full back up tapes are labeled, placed in the storage container and subsequently picked up by storage company personnel and taken to the storage facility.
- Each week thereafter, on Tuesday, a storage box is returned to the USOE to accommodate the differential and incremental tapes. On Monday through Thursday the backups start at 5:00 p.m. and complete by 1:00 or 2:00 a.m. The incremental backup is done in the early hours of Saturday morning (12:00 a.m.) This process repeats for the remaining weeks of the month and at the end of the month the full backup process starts again.
- The process is repeated each month.

TAPE BACKUP SCHEDULE
Figure 1



Note: Using the above example, there would be FIVE labels for the month as follows:

A1 MONTH_YEAR FULL
B2 MONTH_YEAR DIFF & INCR
B3 MONTH_YEAR & INCR
B4 MONTH_YEAR & INCR
A1 MONTH_YEAR FULL

The letter signifies the set, so there are four different sets listed. The number identifies the slot where the tape was located in the tape backup device. If more than one tape is used for a backup, they would be labeled as follows: **A1** MONTH_YEAR **FULL**, **A2** MONTH_YEAR **FULL**, **A3** MONTH_YEAR **FULL**; or

Currently, a Dell Server configured with Windows 2000 Advanced Server with Veritas Backup Exec, Version 8.6 build 3878 is being used for the backup process. It is connected via SCSI to an ADIC FastStor, Model DA-DLT-7000, and Part #62-0124-01. DLT media is used in the tape drive.

The above configuration would be required to replace the system if necessary.

The Veritas support telephone number is 1-800-634-4747 or 1-407-531-7200. The USOE Contract ID is 7315-3051-1624, VIP Agreement #0000003418 and VIP customer #48187. The activation code for Backup Exec Remote Agent NT/2000 is 08-7373-9994-000900. The activation code for Backup Exec Remote Agent NT/2000 is 01-4717-9997-003969, which activates 23 remote agents. The Backup Exec IDR Server and remote activation codes are 04-4898-9994-000535, 04-7230-9998-002231.

An electronic log of the tapes in the individual boxes is kept off site at the perpetual storage company. The electronic log can be found at \\begroups\acs$\backup logs.xls. A printed copy of the log is placed in the box with the tapes. Tapes are identified by box # and month.

Example:

BOX #	1425

Month	Month-03

ACS Tapes	
	A1 Month 2003 Full
	A2 Month 2003 Full
	A3 Month 2003 Full
	A4 Month 2003 Full

Jobs are labeled with the server name and the type of backup such as: BEAIMS DIFF, BEAIMS FULL, and BEAIMS DIFF & INCR. These jobs are located in the Backup Exec software; and are custom jobs that the software user could set up.

BEAIMS DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
System State is backed up in its entirety

BEASEPRD DIFF

C$ is backed up in its entirety
E$ is backed up in its entirety
F$ is backed up in its entirety
System State is backed up in its entirety

BECERT DIFF

C$ is backed up in its entirety
E$ is backed up in its entirety
F$ is backed up in its entirety
G$ is backed up in its entirety

BECOGNOS DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
System State is backed up in its entirety

BEDC13 DIFF

C$ is backed up in its entirety
System State is backed up in its entirety

BEDC14 DIFF

C$ is backed up in its entirety
System State is backed up in its entirety

BEDNS2 DIFF

C$ is backed up in its entirety
System State is backed up in its entirety

BEDRIRIS2 DIFF

C$ is backed up in its entirety, with exception no backup done on Timbuk2
E$ is backed up in its entirety
F$ is backed up in its entirety
System State is backed up in its entirety

BEEASERV DIFF

C$ is backed up in its entirety

D$ is backed up in its entirety
System State is backed up in its entirety

BEEBRIGHT DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
E$ is backed up in its entirety.
System State is backed up in its entirety

BEGROUPS DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
System State is backed up in its entirety

BEIMC DIFF

C$ is backed up in its entirety
System State is backed up in its entirety

BENTBKUP2 DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety, with exception no backup done on images, and images$.
System State is backed up in its entirety

BEPS1 DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
System State is backed up in its entiret

BEPS2 DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
System State is backed up in its entirety

BESYBASE1 DIFF

C$ is backed up in its entirety
E$ is backed up in its entirety
F$ is backed up in its entirety

BETERM DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
System State is backed up in its entirety

BEUSOE1 DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
System State is backed up in its entirety

BEWEB DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
System State is backed up in its entirety

ALOGAN DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
System State is backed up in its entirety

THEBER DIFF

C$ is backed up in its entirety
D$ is backed up in its entirety
System State is backed up in its entirety

APPENDIX L

RECOVERY OF LOST DATA AND HARDWARE

1. RECOVERY OF LOST DATA AND SOFTWARE

1.1 Lost data and software will usually be recovered by a network administrator from backup tapes.
From now on any reference to lost data or recovery of data also implies loss or recovery of software (programs). All network servers are incrementally backed-up on a nightly basis with full system backups occurring during the weekend preceding the first Tuesday. The full system backup just completed plus the incremental backup tape set from the month just ended is picked up by Perpetual Storage for offsite storage on this Tuesday. In some cases, LAN policies, procedures, and installation notes are backed-up separately on diskette or smaller tape backup devices. This allows the recovery of the systems needed to "boot strap" the LAN and restore recovery subsystems. Also, some larger databases are not included in the incremental schedule since they would cause too much nightly volume. All users are encouraged to save any data worth backing-up on network devices to take advantage of these tape backups. Individual "local" client drives are not backed-up unless the user does so on his or her own and employs diskettes or a standalone tape backup sub-system.

An offsite tape set is kept at the offsite storage location for one year. When the month corresponding to the one on the tape set is passed in the next calendar year that set is returned to the USOE and recycled one time as full-system or incremental tapes. When they make their way back to the USOE the second time from offsite storage they are discarded. The exceptions to this are the July tape sets. They are kept offsite indefinitely (at lease 5 years). If tape backup systems change, care must be taken to insure that tapes backed up before the system change can still be retrieved. Two incremental tape sets are created during the course of one "back-up month". The first is started on the Monday preceding the first Tuesday of the month. It is kept in the drive for two weeks. On the second Monday following the first Tuesday, this first incremental backup set is removed and placed in the safe and a second incremental backup for the month is begun. Both incremental backup tape sets are sent off-site with the full-backup set for the new month on the first Tuesday of the new month.

If it is necessary to recover any files from tapes in off-site storage Perpetual Storage will deliver any needed tape sets within 90 minutes for approximately $24.00. You will usually get a given month's full-backup and the preceding month's incremental backups in the same safe box. You must specify which month's or months' boxes you need based on the restoration needs of the user. In some cases both full and incremental sets will be needed. Once a box of tape sets is returned to the USOE it will be kept on-site in the safe until the first Tuesday of the following month, at which time it will be returned to Perpetual Storage unless its one year in off-site storage has passed.

1.2 Using the Conner backup/restore software, restore procedures may be performed for any server. Entire volumes (disk drive or disk array sub-system) may be restored as well as selected directories or individual files within a volume.

1.3 The amount of time required for any recovery will vary greatly depending the volume of data lost, and how long ago the loss occurred. A full volume lost at the end of the month would require the recovery of the first of the month's full volume backup as well as any incremental backups which took place on intervening days.

1.4 In the event of catastrophic loss of data such as in a fire, flood or earthquake, the first useable full system tape backup set must be determined. If the current (last written) full system tape backup set were onsite and useable, then that set would be used, otherwise the most current set stored offsite by Perpetual Storage would be used. Offsite tapes are retrievable within 1.5 hours. Following the restoration of the most recent available full system backup, any incremental backups which are intact and followed that backup should also be applied. Backups of specialized servers such as teacher certification's imaging system also need to be reviewed. It is believed that at this time their optical diskettes are also being kept off-site at an employee's home.

1.5 The estimated amount of time needed to recover the most current recoverable data in a worst case situation is 12 hours and would require the services of only one lan administrator. However, if the most current recoverable media is old (for example, a month or two) considerable time and effort will be needed to manually recover parts of the data. If any hardware necessary for recovery needs to be replaced before data recovery, that process would have to occur first. These procedures are discussed in the next section.

2. RECOVERY OF HARDWARE

2.1 The following is an analysis of the time required to restore agency hardware to the state it was in before the disaster. It assumes a worst case scenario in which all hardware within the building, including the entire LAN room has been lost and must be replaced. Estimates of time and costs necessary for a "partial" disaster could be inferred from this information. Depending on the nature of the disaster which caused loss of hardware the activities described below may have to take place in a new or temporary facility.

With the exception of the LAN room the assumption is made that all necessary telecommunications wiring (PBX, data-circuits, wiring panels, and jacks) are in place and functional. If this is not the case additional time (anywhere from a few days to a few weeks) will be needed to install these network components. Currently US West is running at least 60 days behind on installations. US West could take at least 30 days to install any new circuits unless we could get them to escalate our order. If we were dealing with a large earthquake this could be much longer. In any event outside communications may take much longer to establish than restoration of services within the agency.

2.1.1 Rewiring of the LAN room in order to accommodate pre-disaster hardware would require about 8 hours of work. This assumes assistance from an ITS wiring crew which would help with connections to telecommunications panels and circuits.

2.1.2 Each device which makes up the LAN room component of the network will have to be reinstalled and configured. The following list addresses each type of device and attempts to estimate the average amount of time to reinstall and configure such a device. These times are then multiplied by the number of devices to come up with a total amount of time needed to reinstall and configure all such devices.

Note that reinstallation cannot begin until at least some of the replacement devices have been ordered and delivered. Usually machines can be ordered and delivered within seven working days. To complete a large order could take considerably longer. Total recovery cannot be completed until all replacement hardware has been delivered. It has been recommended that Risk Management be approached with the suggestion that they keep some spare servers on hand for use by any state agency needing replacements thus expediting this process. Note that time needed includes hardware configuration as well as installation of any system software not available from tape backup restores.

TYPE OF DEVICE	TIME NEEDED	UNITS	TOTAL TIME
Novell servers	5 hours	9	45 hours
(subsystems such as disk arrays factored into estimate)			
Unix servers	8 hours	1	8 hours
Tape backup system	9 hours	1	9 hours
(Includes server & Carousel)			
Concentrators	5 mins	40	4 hours
Ether-switch	2 hours	1	2 hours
Routers	2 hours	2	4 hours
Imaging System	2 days (informational, responsibility of Comgraphix)		
Miscellaneous	10 hours		10 hours
		TOTAL	82 hours

2.1.3 In a worst case scenario all desktop client machines and network printers would also need to be replaced. The time necessary for the installation of each machine, which includes unpacking, assembly (including any special hardware installation) and software installation and configuration is estimated to be 1 hour per machine. This amounts to a total of 43 (340 / 8) man work days given approximately 340 desktop machines and printers. Any standalone software/data recovery (from backup diskettes or tape) which needs to be done for desktop machines will be the responsibility of the user of that machine.

2.1.4 To estimate the total elapsed time necessary for recovery of all hardware to its pre-disaster state we need to consider: number and type of available staff, length of work week, actual time on task, and unforseen contingencies.

2.1.4.1 There are two staff members available for recovery of LAN room hardware. It is possible that two USOR (Dewey Dipoma, Abdul Matin) and one DCS (Mike Wilde) LAN administration specialists may also be able to assist in LAN room recovery as well as with recovery of desktop machines. This would depend on obligations to their respective sections. Having up to three additional persons would speed up this process as would acquiring help from outside computer consultants. However we will see in the desktop discussion below that assignments of staff needs to be balanced between LAN room and desktop tasks.

2.1.4.2 Regardless of the number of qualified staff available the estimated 82 hours need to be adjusted upward by some factor to account for: planning, actual time on task and unanticipated problems. For the purposes of this analysis we will set this factor at 1.4. Thus the real hours needed to recover hardware is 115 hours. Dividing this by two LAN specialists yields approximately 60 hours or 6 and ½ work

days. Adding this to the 12 hours estimated for recovery of software and data from tape gives approximately 8 or more elapsed work days. We cannot divide data and software recovery time by 2 persons, since we have only one backup/restore system. However it is possible that data and software recovery could begin before all servers are recovered thus saving some total elapsed time.

2.1.4.3 Finally we need to consider how much total elapsed time would be necessary for the replacement/recovery of desktop machines. While the LAN room hardware is being recovered it may be feasible that programming staff, LAN zone leaders (part-time "power users") and some of the DCS or USOR LAN specialists, could install and recover the desktop machines throughout the building. This may require some initial training (a few hours) from the LAN administration staff who are recovering the LAN room hardware and the ACS Macintosh specialist. Above we estimated 43 work days for recovery of desktop machines. Multiplying this by our 1.4 factor and dividing by an expected 7 staff members we come up with 8.6 work days. The above applies to only computer hardware and not to other office equipment.

Since this activity can proceed concurrently (with the exception of server connection testing) with the LAN room hardware recovery; and since its elapsed time for completion is approximately the same (8.6 work days verses 8+ workdays) we have both major hardware recovery activities finishing in approximately two work weeks. Of course this timetable could be accelerated through longer hours and/or outside help. Also, unskilled agency staff could be used to help unbox equipment, move it into place and plug them into power strips.

3. COSTS OF HARDWARE RECOVERY

3.1 The following is a table which estimates the cost of replacing all the hardware within the Utah State Office of Education. These costs are based on rounded estimates of the number of units of various hardware as well as current replacement costs. Funding of such replacements will not be discussed at this time. The assumption is that State Insurance/Risk Management would cover most of this loss.