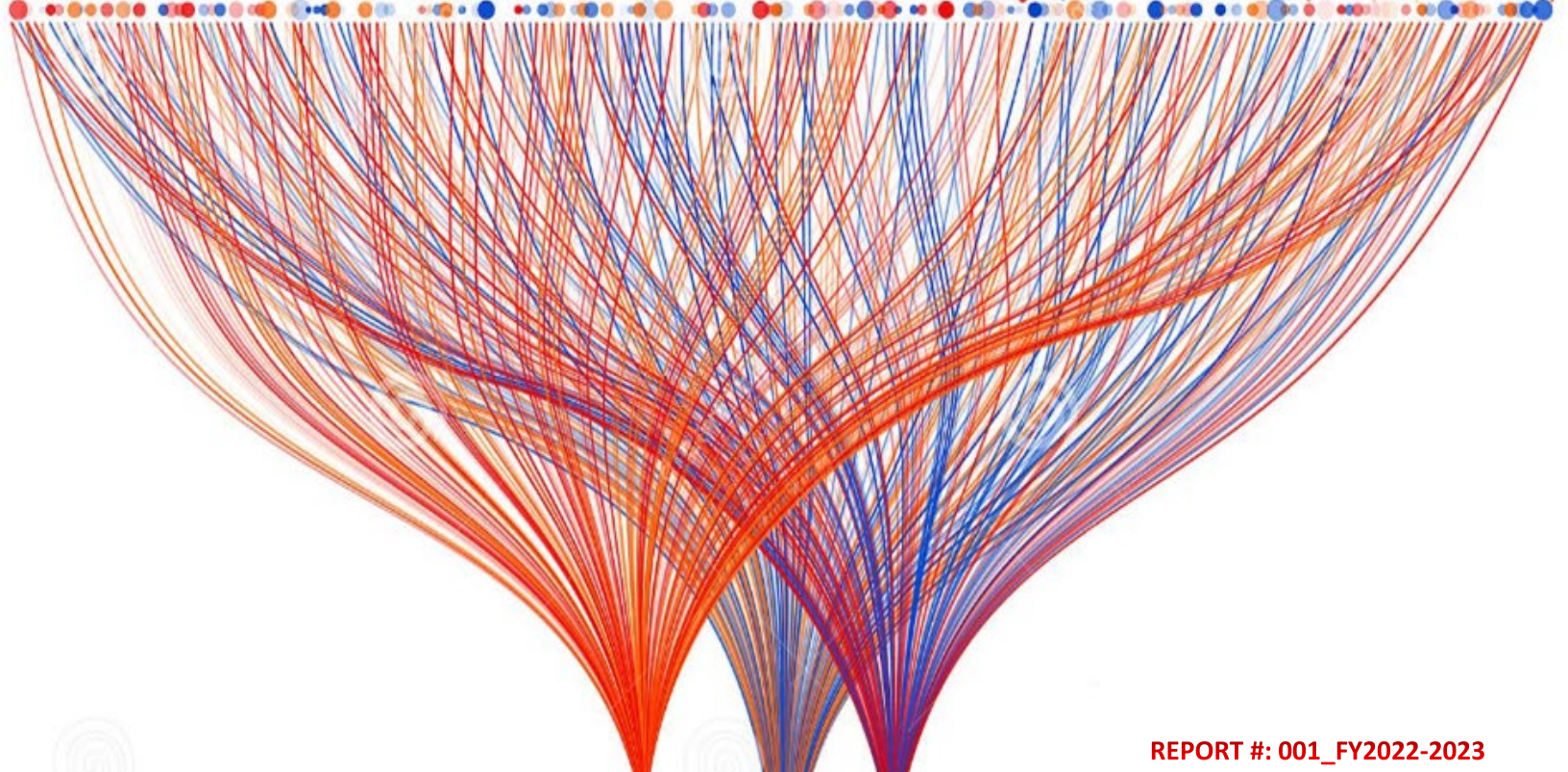




OFFICE OF INTERNAL AUDIT

AUGUST 31, 2022

Technology Services (TS) Department: Disaster Recovery Plan & Business Continuity Plan



REPORT #: 001_FY2022-2023

MARTHA SMITH
INTERNAL AUDITOR



TABLE OF CONTENT

PAGE

Executive Summary iii

Overview:

Background	1
Statement of Auditing Standards	5
Audit Due Professional Care and Inherent Risk	5
Audit Scope	5
Audit Purpose and Objectives	5
Audit Methodology	6
Exclusions	6

Observations:

1- No Departmental Policies and Procedures for DR and/or BC	6
2- Limited Information and Content in TS's DRP/BCP	7
3- No Written TS DRP/BCP for Essential District Departments	11
4- Undifferentiated DRP and BCP Processes and Procedures	12
5- TS's DRP/BCP Manual Lacks Foundational Core Principles	13
6- No Management Resolutions to Findings in New External Test Report	14
7- Un-Implemented Management Responses and Corrections (MRC's) from Consultation Audit	15
8- Restrictions and Delayed Access to Information	16
9- Incomplete Business Impact Analysis (BIA) Report	16
10- Vague DRP/BCP Standard Operating Procedures	20
11- Variations Between Devices Listed in the Supporting Data and TS's DRP/BCP Manual	21
12- Results in TS's Backup Log	21
13- Oversights in TS's DRP/BCP Manual	22

Conclusion 23

Acknowledgment 23

Appendix A: Exhibits 25

Appendix B: References 27

Appendix C: Glossary 35

The Office of Internal Audit (OIA) has completed the compliance audit of the Technology Services (TS) Department's Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP). This audit was scheduled on the annual risk assessment plan for School Year (SY) 2022/2023. A previous consultation audit of the TS DRP/BCP was completed on June 30, 2021. A copy of the consultation's final audit report was delivered to the District's Executive Management, and an Executive Summary of the consultation was provided to the Governing Board on June 30, 2021. The conclusion sections of the consultation audit report noted that a new assurance audit would be conducted in approximately twelve months from the issuance date of the final consultation audit report.

The purpose of this compliance audit was to determine:

- 1- The compliance of the TS DRP/BCP manual with existing guidelines.
- 2- Its readiness to manage an occurrence in an effective and efficient manner -prior to, during, and after a disaster- using the provided TS's DRP/BCP manual and data.
- 3- The progress on the implemented Management Responses and Corrections (MRCs) from the consultation audit finalized on June 30, 2021.

This compliance audit is a review of TS's DRP/BCP manual and supporting data; it does not reflect or discount the effectiveness of the TS management or its staff. The current TS management and staff have proven themselves capable of, and qualified to, get through an unforeseen dramatic event.

Simply stated, lesser experienced or lesser qualified staff members would need to rely on implementing the standard procedures and processes of the TS DRP/BCP manual. Therefore, the manual's content should be sufficient to guide others through future unforeseeable catastrophes, that could include, the current TS management and staff being unavailable.

Internal Audit assessed the requested and provided TS DRP/BCP materials, which contained, their updated DRP/BCP manual, District policies, TS's standard operating procedures, and specified reports. This audit also reviewed the MRCs from the previous consultation audit.

The audit scope encompassed information from July 1, 2021, through June 30, 2022.

The objectives of this assessment were similar to the previous consultation audit, with some necessary adjustments to accommodate requested limitations by the TS department.

The audit objectives were achieved by reviewing provided copies of requested preliminary items uploaded by TS into a shared Microsoft Teams folder. The TS information was compared to content created by leading organizations, and agencies that develop, review, and issue applicable DRP/BCP standards, policies, procedures, regulations, and guidelines.

Excluded from this audit were DRP/BCP vendor activities, employee duties/responsibilities, site visitations, and unrelated TS DRP/BCP tasks.

Observations are listed below, in order of their perceived risk -highest to lowest- as determined by Internal Audit:

1. NO DEPARTMENTAL POLICIES AND PROCEDURES

Condition: The TS Department does not have written policies and procedures for the Disaster Recovery (DR) and/or Business Continuity (BC).

2. LIMITED INFORMATION AND CONTENT IN TS'S DRP/BCP

Condition: The TS DRP/BCP content is limited, and it is missing basic DRP/BCP elements.

- 3. NO WRITTEN TS DRP/BCP FOR ESSENTIAL DISTRICT DEPARTMENTS**
Condition: TS's DRP/BCP manual does not include or identify essential district departments and their key procedures.
- 4. UNDIFFERENTIATED DRP AND BCP PROCESSES, PROCEDURES, AND RESPONSIBILITIES**
Condition: The TS DRP/BCP does not differentiate between working through a disaster versus recovering from a disaster.
- 5. TS'S DRP/BCP MANUAL LACKS FOUNDATIONAL CORE PRINCIPLES**
CONDITION: The TS DRP/BCP manual does not disclose what basic core principles and/or fundamentals were followed to create the department's manual.
- 6. NO MANAGEMENT RESOLUTIONS TO THE FINDINGS OF THE EXTERNAL TEST REPORT**
CONDITION: The recently provided external test report, dated February 3, 2022, did not contain management's responses or scheduled corrections to the findings.
- 7. UN-IMPLEMENTED MANAGEMENT RESPONSES AND CORRECTIONS (MRC'S) FROM CONSULTATION AUDIT**
CONDITION: Specific to the previous Consultation Audit, some progress on the recommended and provided MRC's has been made.
- 8. RESTRICTION AND DELAYED ACCESS TO INFORMATION**
CONDITION: TS created delays on requested preliminary documents, requested extensions, re-schedules, and requested audit limitations.
- 9. BUSINESS IMPACT ANALYSIS (BIA) REPORT**
CONDITION: The provided BIA document was missing key elements commonly found in a BIA report.
- 10. VAGUE DRP/BCP STANDARD OPERATING PROCEDURES**
CONDITION: Standard Operating Procedures (SOP) for DRP/BCP do not provide sufficient guidance or instructions.
- 11. VARIATIONS BETWEEN DEVICES LISTED IN THE SUPPORTING DATA AND TS'S DRP/BCP MANUAL**
CONDITION: Some devices listed in the TS DRP/BCP manual -Section VIII -Network Infrastructure were not included in the supporting data.
- 12. RESULTS IN TS'S BACKUP LOG**
Condition: No explanation or corrections for, failed jobs and failed objectives in the provided "BackupLog-Physical Virtual2-July2022".
- 13. OVERSIGHTS IN TS'S DRP MANUAL**
Condition: The DRP Manual for the IT Department contains several changes, undisclosed reference, and oversights.

BACKGROUND

The Technology Service Department (TS), for the Tucson Unified School District (District), "...is committed to enhancing and improving the District's technology resources and support at all of the District's schools on an equitable basis. The data network we support extends over 250 square miles and serves approximately 43,000 students and 8,300 staff. Our network is one of the largest in the state."¹

The District's TS Department is responsible for one of the largest school networks in the state; the District is comprised of 89 schools K-12, plus educational programs and administrative departments.

The mission of the District is "...in partnership with parents and the greater community, is to assure each pre-K through 12th grade student receives an engaging, rigorous and comprehensive education. The District is committed to inclusion and non-discrimination in all District activities. At all times, District staff should work to ensure that staff, parents, students, and members of the public are included and welcome to participate in District activities."²

The department supports, maintains, and provides solutions while ensuring a safe and secure infrastructure. TS ensures the District's end users experience minimal disruption during daily activities by managing various mediums of communication between applications/software, providers, vendors, and other parties.

On June 30, 2021, a consultation audit was performed and completed of the TS Department's Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).

The consultation audit was originally intended to be an assurance audit. During the preliminary stages of the audit, the scheduled audit was converted into a consultation audit. The change was viewed as an opportunity to add value to management's efforts. The change was discussed and agreed to by TS's Chief Technology Officer (CTO) and Information Technology Director (Director) on February 8, 2021.

The Institute of Internal Audit (IIA) classifies internal audits as either *assurance* or *consultation*. The main difference between them is their level of risk, management's involvement during the audit process, and the distribution of the final report.

IIA definitions:

Assurance audits are "An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements."³ These audits have a systematic format, minimal flexibility, and require Management's Response and Commitments (MRCs) to audit observations.

Consultation audits are "Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training."⁴ These audits have a flexible format to allow feedback from

management during the audit process, and a collaborated effort on the corrections of the audit findings. No MRC's are required; however, if management decides to provide them, they become part of the final audit report.

Regardless of the type of internal audit, the IIA performance and implementation standards should be followed when analyzing organizational controls, governance, and risk management.

After a consultation audit, it is common practice to schedule and perform an assurance audit. The schedule for the upcoming assessment audit is discussed and agreed upon with management during the exit meeting.

During the exit meeting of the consultation audit, July of 2022 was selected by TS's Executive Management, and agreed upon by Internal Audit, as the date to conduct the assessment audit of the TS DRP/BCP.

Notification of this assurance audit was documented in the conclusions of the final consultation audit report, which read "An assessment audit of the IT DRBCP will be scheduled for approximately one year from the date this final report is delivered to the Superintendent". The report was delivered to the Superintendent on June 30, 2021. This audit was also scheduled in the provided Annual Internal Audit Plan (Audit Plan) for a specified School Year (SY) 2022-2023. The Audit Plan is a worksheet that includes a list of audits and their estimated schedule to be performed during the upcoming SY. The Audit Plan for SY 2022-2022 was e-mailed to the Governing Board, Audit Committee, and Executive Leadership on May 13, 2022. The Audit Plan was also presented during the Audit Committee's public meeting on May 20, 2022, in which TS executive managers were present.

The focus of this audit was to review TS's processes and procedures regarding DRP/BCP; it was not intended to reflect or discount the effectiveness or abilities of the TS management or its staff. It is noteworthy to acknowledge that the current TS management and staff have demonstrated and proven themselves capable of navigating the District through an unforeseeable pandemic.

Nonetheless, capabilities and qualifications of the current TS team does not eliminate the need to have a comprehensive TS DRP/BCP manual, policies, procedures, and standards for the department. Having a DRP/BCP is a preventative measure to aid recovery and/or maintain operations in case of future unforeseeable catastrophes. It is possible that a future event may include the current TS management and/or staff members being unavailable.

Terminology: The terms DRP and BCP are sometimes used synonymously by organizations with minimum distinctions between their activities and requirements. Not identifying pertinent activities and processes in each of these plans creates gaps in their executions and effectiveness.

The DRP is sometimes referred to as an Emergency Operations Plan (EOP), or Enterprise Backup & Recovery Plan (EBRP). The BCP is referred to as a Business Continuity Management (BCM), Business Process Continuity (BPC), and/or Continuity of Operations Plan (COOP).

The diagram below, obtained from the Office of the Arizona Auditor General (AZ Auditor), displays the DRP and BCP as two separate plans stemming from "Incident Management".



IMAGE FROM THE AUDIT GENERAL RISK AND BUSINESS CONTINGENCY PLANNING⁵

Having individual DRP’s and BCP’s, with identifiable responsibilities, enhances the organizations efficiency and effectiveness of operation by eliminating potential tasks that could be overlooked during chaos.

This audit will refer the DRP and BCP as two separate plans while noting some interconnected activities. References of DRP and BCP utilized in this report were focused, whenever possible, on criteria and policies related to technology services, education (K-12), and combinations thereof.

The Information Systems Audit and Control Association (ISACA), formal definitions of a Disaster Recovery (DR) and Business Continuity (BC), are:

“Disaster Recovery (DR): Activities and programs designed to return the enterprise to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan (DRP) to restore an enterprise's critical business functions.”⁶

“Business Continuity Plan (BCP): A plan used by an enterprise to respond to disruption of critical business processes. An organization depends on the contingency plan for restoration of critical systems.”⁷



AUDITING BCP PONDURANCE ISACA PRESENTATION⁸

The National Institute of Standards and Technology (NIST) is the federal government guiding document for Informatics and Information Technology (I&IT); its series document 800-34 addresses the required guidelines and provides a more comprehensive definition of DRP and a BCP. (NIST’s *guidelines are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130*).

NIST specifies, “The DRP applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. The DRP may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established. A DRP may support a BCP or COOP plan by recovering supporting systems for mission/business processes or mission essential functions at an alternate location. The DRP only addresses information system disruptions that require relocation.”⁹

NIST states, “The BCP focuses on sustaining an organization’s mission/business processes during and after a disruption. An example of a mission/business process may be an organization’s payroll process or customer service process. A BCP may be written for mission/business processes within a single business unit or may address the entire organization’s processes. The BCP may also be scoped to address only the functions deemed to be priorities. A BCP may be used for long-term recovery in conjunction with the COOP plan, allowing for additional functions to come online as resources or time allow. Because mission/business processes use information systems (ISs), the business continuity planner must coordinate with information system owners to ensure that the BCP expectations and IS capabilities are matched.”¹⁰

According to TechTarget, “Disaster recovery (DR) and business continuity planning are often linked, but they are different. A DR plan is reactive, as it details how an organization recovers after a business disruption. A business continuity plan is a proactive approach that describes how an organization can maintain business operations during an emergency.”¹¹

Simply stated, and regardless of the acronym used, each plan has specific functions. DRP focuses on restoring data access and IT infrastructure after a disaster. BCP focuses on keeping business operational during a disaster.

The AZ Auditor General goes even further, as to eliminate the guess work, by providing steps in the process their agency would find acceptable for an organization to have in its contingency plan. Starting with the fundamental steps of developing a written policy.



IMAGE IS FROM THE AUDIT GENERAL RISK AND BUSINESS CONTINGENCY PLANNING ¹²

STATEMENT OF AUDITING STANDARDS

Internal Audit used IIA standards as a guide, along with the research performed on DRP/BCP from leading organizations entrusted with writing guidelines, responding to occurrences, and performing assessments, such as: Arizona Auditor General (AZ Auditor), Information Systems Audit and Control Association (ISACA), National Institute of Standards and Technology (NIST), Federal Information System Controls Audit Manual (FISCAM), International Organization for Standardization (ISO), Arizona Strategic Enterprise Technology (ASET) Office, U.S. Government Accountability Office (GAO), Government Auditing Standards (GAS), and the Department of Education (DOE).

Additional research was conducted for applicable DRP and BCP District policies, procedures, and acceptable industry practices and regulations regarding technology services departments in school districts with similar student populations throughout the nation.

Audit Due Professional Care and Inherent Risk

Audits are designed to add value; this can be done with participation and collaboration from all levels of management.

All audits contain an element of inherent risk; this is a limitation with countless reasons. Audits can only evaluate, analyze, and develop conclusions and recommendations on accessed District's internal data, applicable records, and collaboration from management and leadership.

Due Professional Care implies reasonable care and competence, not infallibility.

Internal audits are conducted to provide management with reasonable –not absolute- assurance that the organization's objectives will be met.

AUDIT SCOPE

The scope for this assurance audit is from July 1, 2021, through June 30, 2022. The internal audit activities were concentrated on reviewing the content of TS's DR and BC manual, and supporting documents.

AUDIT PURPOSE AND OBJECTIVES

The purpose of the audit was to provide an independent and objective assessment of the department's DRP/BCP manual. And to verify the implementation of agreed upon MRC's from the previously performed consultation audit.

The set objectives of this audit were to evaluate the department's DRP/BCP to determine compliance of its DRP/BCP's manual, efficiency, and effectiveness.

Audit objectives were achieved by analyzing and reviewing the following documents:

- a- TS's DRP/BCP manual.
- b- TS's Processes of the DRP/BCP.
- c- TS's Standard Operating Procedures (SOPs) for DRP/BCP.
- d- TS's Business Impact Analysis.
- e- Existing district policies.
- f- CDW Security Assessment for the District.
- g- Previous consultation audit report and relevant supporting documents.
- h- Research of DRP/BCP for acceptable standards, regulations, and guidelines.

AUDIT METHODOLOGY

Compliance with acceptable DRP/BCP were determined by comparing the requested documents from TS to applicable district polices, acceptable practices, procedures, and research of DRP/BCP standards from governing organizations and agencies.

Effectiveness and efficiencies of DRP/BCP's were determined by evaluating and reviewing the processes, content, and procedures to determine if the steps in the process were functional. Example, during a disaster, would following the processes in TS's DRP/BCP manual result in effective risk management -maintain or restore- operating systems and efficiently re-establish the department and the District's critical functions in an acceptable time frame.

Implementation and completion of observations from the previous consultation audit were accomplished by reviewing and comparing the new TS DRP/BCP manual and information to the corresponding documents analyzed during the previous consultation audit. There were no: in person meetings, testings, or observations of related DRP/BCP processes, practices, performances, or implementations. There were no reviews of TS's DRP/BCP staff responsibilities, department infrastructure, visitations to TS site(s) or the District's disaster recovery and business continuity location(s).

EXCLUSIONS:

TS vendor contracts and activities, employee responsibilities, assignments, and TS's practices and tasks not related to DRP/BCP's.

Audit observations and recommendations are listed below, in the order of their perceived risk, as determined by Internal Audit.

AUDIT OBSERVATIONS AND RECOMMENDATIONS**1. NO DEPARTMENTAL POLICIES AND PROCEDURES**

Condition: The TS Department does not have written policies and procedures for the Disaster Recovery (DR) and/or Business Continuity (BC).

Criteria: Arizona Auditor General (AZ Auditor) states, "While most districts have some IT policies and procedures in place, those policies or procedures may not be comprehensive enough to cover all IT areas or may need to be more formally documented... The following list of policy topics is not intended to be exhaustive, so a district may have additional policy needs. Only after evaluating current systems and processes will a district be able to determine exactly what policies and procedures it needs to help secure its IT resources.

Some policy topics a District should address include the following:

- Data privacy, security, and access to data and systems, including data backup, remote access, and wireless networks.
- General IT security, user password security, device security settings, etc.
- Logging and monitoring of key activities on systems and networks.
- Appropriate use of the internet and District e-mail systems.
- Security and use of student information system.
- Use of accounting information system.
- Specific DR and BC planning (See FAQs #6-9 for more information)."¹³

Effect: The department provide existing District policies pertinent to TS, for the requested DRP/BCP policies; however, the provided policies do not reference DR or BC actions. During the previously conducted consultation audit a questionnaire was performed in which the department’s executive manager response to having a DRP/BCP policy was “...A District Policy formulation update in progress” ¹⁴

Not having departmental or District policies for DRP/BCP will result in the department’s inability to uniformly perform and/or uphold:

- Operational standards.
- Accountability for actions, or lack of.
- Guidance for employees on activities and tasks.
- Governance and direction to its organizational structure.
- Transparency to taxpayers.

Cause: No DRP/BCP policies.

Recommendations:

- a. Create policies, procedures, and processes specific to DRP and BCP.
- b. Correlate DRP/BCP documents with acceptable standards, policies, and procedures.

2. LIMITED INFORMATION AND CONTENT IN TS’S DRP/BCP

Condition: The TS DRP/BCP content is limited and is missing basic DRP/BCP elements.

Criteria: DRP/BCP content may vary depending on the industry and the organization; however, there are commonalities in content and key elements.

“The Arizona State Emergency Response and Recovery Plan (SERRP) is an all-hazards plan addressing Arizona’s hazard and threat environment, including natural, technological, and human caused emergencies or disasters... The plan is designed as a high tier Whole Community document identifying state agency roles and responsibilities during an emergency or disaster.”¹⁵

“NIST Special Publication 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, provides instructions, recommendations, and considerations for federal information system contingency planning. Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.” ¹⁶

Image below, is an example of the Table of Contents from The National Institute of Standards and Technology (NIST) Special Publication 800-184, showing some of common items in a DRP guide.

NIST SP 800-184		GUIDE FOR CYBERSECURITY EVENT RECOVERY	
Table of Contents			
Executive Summary			vi
1. Introduction			1
1.1 Background			1
1.2 Purpose and Scope			2
1.3 Audience			2
1.4 Document Structure			3
2. Planning for Cyber Event Recovery			4
2.1 Enterprise Resiliency			4
2.2 Recovery Planning Prerequisites			6
2.3 Recovery Plan.....			7
2.3.1 Planning Document Development.....			7

17

NIST'S GUIDE FOR CYBERSECURITY EVENT RECOVERY


ISACA's second Information System Recovery Principles states: "Create a Recovery Team with Roles and Responsibilities – The team should include all the functions and roles necessary to quickly and completely restore computer operations. There should be a document that identifies the team members, their respective roles and the steps each would take in restoring operations."¹⁸

AZ Auditor states "The items necessary for each plan may vary by entity, but some basic DRP components include the following:

- Identification of critical equipment, data, and resources, including off-site locations to store backup data and maintain redundant system resources to allow for emergency data processing.
- Contact list of key individuals including their roles and responsibilities.
- Procedures for regularly backing up systems and data, and regularly testing backups.
- Procedures for activating the DRP, notifying appropriate parties, and assessing the severity of the disruption and the required response.
- Steps and procedures for restoring systems to full functionality.
- Supporting information as necessary to ensure a comprehensive plan such as business impact analysis, vendor contract information, etc."¹⁹

Effect: DRP/BCP's are meant to be a comprehensive guide on how to act, coordinate, and navigate through an incident. TS's DRP/BCP document does not include basic content such as: Scope, purposes, processes, team responsibilities, and procedures to guide the department, prior to, during, or after a disaster.

Image of TS’s DRP/BCP Table of Content:



TUCSON UNIFIED
SCHOOL DISTRICT

Contents

I.	Overview.....	3
II.	Document Maintenance and Update Requirement	3
III.	Disaster Event Declaration	3
IV.	Disaster Recovery (DR) & Business Continuity (BC) Team Members and Escalation List.....	4
V.	Accessing Vital Records	7
VI.	Systems In-Scope, Recovery Point Objective (RPO), Recovery Time Objective (RTO) & Tiers .	12
A.	Definition.....	8
B.	Tiers	8
VII.	Redundancy through Backup and Replication.....	9
VIII.	Network Infrastructure Failover Procedure	9

TS’s DRP/BCP TABLE OF CONTENT ²⁰

The Arizona Department of Education quoted the NIMS’s five mission areas of its National Preparedness Goal, in the context of schools, indicating the need for “a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective actions in an effort to ensure effective coordination during incident response.”²¹

While the list below is not all inclusive, it does denote some of the items missing in TS’s DRP/BCP.



THE PREPAREDNESS CYCLE BY AZED ²²

- a) Content regarding actions to be performed, prior, during, and after a disaster, not found in TS’s DRP/BCP manual:
 - Preparedness and prevention tasks necessary to minimize impact from an occurrence, such as ensuring equipment is affixed, generators are functional, etc.

- Protections and procedures to be performed to protect staff and infrastructure (e.g., hardware and software components).
 - Mitigation, necessary measures to minimize or eliminate losses/damages.
 - Response, stabilizing a situation, establishing a safe environment, facilitating, and coordinating processes.
 - Recovery, essential activities for the department's operation.
- b) No listed responsibilities, and specified roles associated with DRP/BCP.
- Operational call tree, as recommended by the AZ Auditor General.

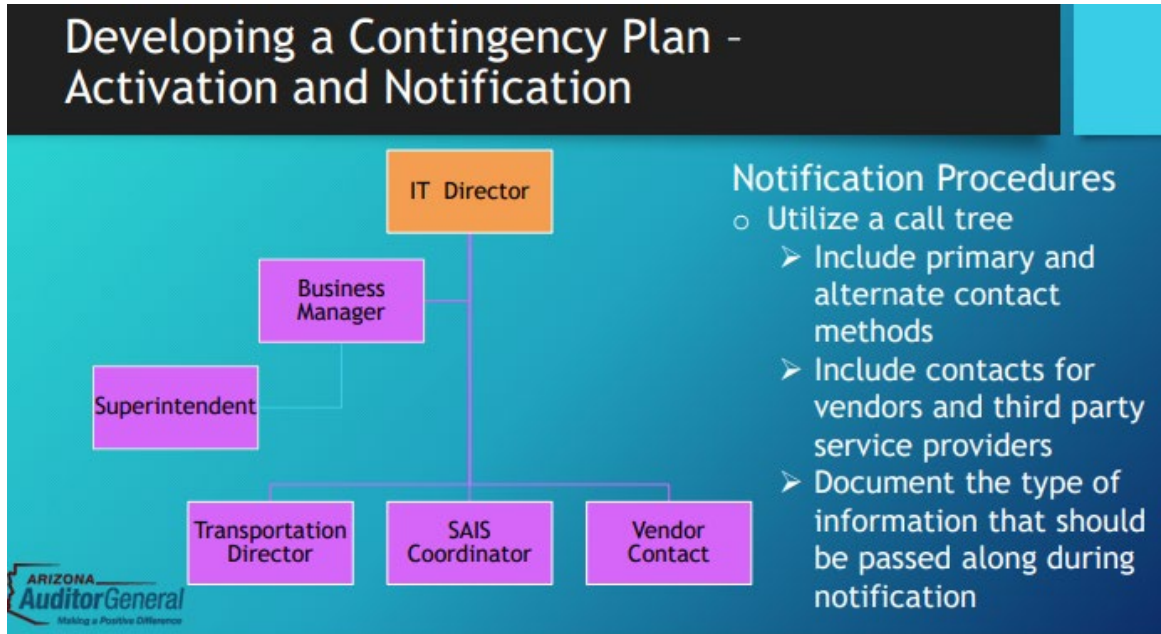


IMAGE IS FROM THE AZ AUDITOR GENERAL RISK AND BUSINESS CONTINGENCY PLANNING²³

- Identified or disclosed external drivers, impact categories, identified key operational risk, vulnerability & disruption analysis.
- No list of District departments and identified vital operating systems.

An unclear DRP/BCP that is missing essential procedures and processes will decrease the efficiency and success of a DRP/BCP. Unclear sentences included in the DRP/BCP, such as “The DR & BC team member who dials in first will setup an instant meeting room via the portal.”²⁴ This sentence does not reflect a well thought out and strategically designed plan.

A common statement shared by Executive Management during the consultation audit was “We know what we are doing”. This statement is addressed by ISACA, who recommends that certain manuals, including technical ones, are meant to be accessible during a disaster. “These manuals are needed because members of the recovery team may not normally do some of the business processes.”²⁵

The ISACA statement is echoed by the sentence, in the background section of this report, which acknowledged the TS’s current ability and qualifications to manage a disaster.

Cause: Internal audit was informed by TS’s management that the TS DRP/BCP was written for TS’s current staff; the document’s content reflects this sentiment since it does not take into consideration that the current TS staff might not be available during a future unforeseeable disaster.

Recommendations:

- a. Update to include required and/or missing information.
- b. Provide the fundamental principles that TS’s DRP/BCP is based on.
- c. Reference sources for images used in the DRP/BCP document.
- d. Identify the purpose and scope in TS DRP/BCP.
- e. Indicate which individuals listed on the DRP/BCP tables are to be contacted.
- f. Classify and identify general responsibilities of each DRP/BCP team member.
- g. Create clear notification procedures, as suggested by the AZ Auditor’s Contingency Planning.

3. NO WRITTEN TS DRP/BCP FOR ESSENTIAL DISTRICT DEPARTMENTS

Condition: TS’s DRP/BCP manual does not include or identify essential departments and their key procedures.

Criteria: AZed, Emergency Operation Planning (EOP)/Continuity of Operations Planning (COOP), references the Arizona School Emergency Operations Plans (EOP)- EOP Minimum Requirements – Arizona Revised Statutes (ARS) 15-341 (A) (31) -Introductions- “...ADE, AZDEMA, Department of Health Services (AZDHS), and the Arizona Department of Public Safety (AZDPS) recognizes a national 6-step process of plan development, as outlined in the two aforementioned national resource documents. Image/Figure 1 depicts the six steps in the planning process...” (Image below).²⁶



ARIZONA DEPARTMENT OF EDUCATION, - ARIZONA SCHOOL EMERGENCY OPERATIONS PLANS (EOP)²⁷

The TS Department is limiting its effectiveness by not having a general TS overview of processes for key departments. During a disaster, there are no guarantees that current

members of the TS DR team would be available, or that other technicians (experienced or not) would be familiar with the District's infrastructure.

Effect: Lack of knowledge of critical activities will prevent TS from effectively and efficiently implement and execute DRP and BCP functions. TS's DRP/BCP reads, "Impacts and related actions resulting from an existing district extend well beyond the needs and actions of the IT team and IT systems. Actions could include providing temporary workspace, relocating key employees and initiating emergency evacuation procedures. These actions and the TS DRP & BCP are part of a larger District-wide DRP & BCP."²⁸ However, the District does not have existing DRP and/or BCP guidelines.

Not having a list of critical processes for key District departments will reduce TS's ability to respond effectively and efficiently during a disaster, diminishing recovery and continuity of operations.

Cause: TS has not conducted a collaborated effort to identify departments essential functions required for TS to re-establish so departments may resume their daily activities.

Recommendation:

- a. Create, in collaboration with essential departments, a comprehensive recovery and continuity plan that identifies and includes a list of the departments' critical functions and processes, while identifying the interconnectivities within the TS structure.
- b. Identify essential departments and their key operating activities.

4. UNDIFFERENTIATED DRP AND BCP PROCESSES AND PROCEDURES

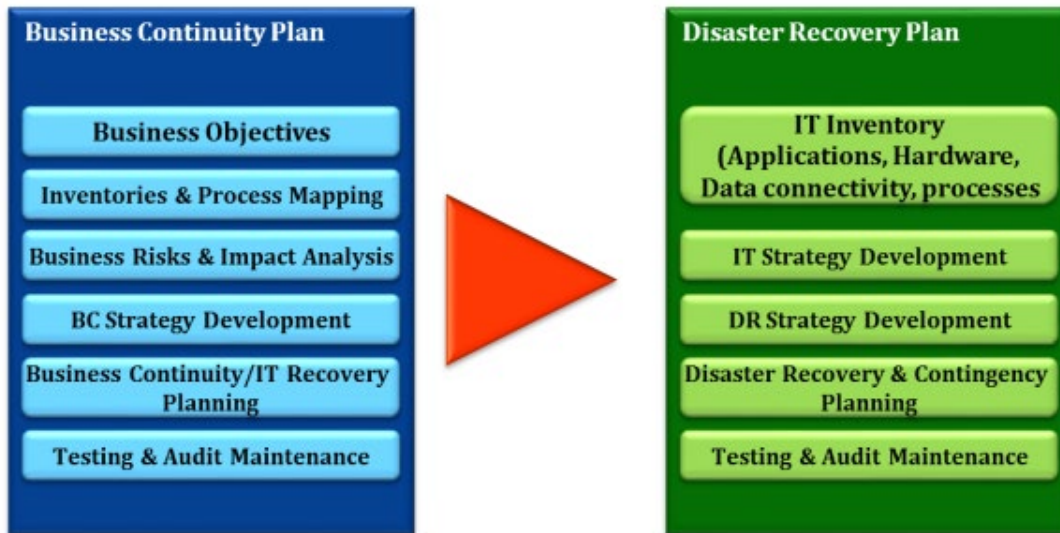
Condition: The TS DRP/BCP does not differentiate between dealing with a disaster versus recovering from a disaster.

Criteria: Global Technology Audit Guide (GTAG) -Business Continuity Management – (Page 3) - 2.3 Disaster Recovery of IT, states "Disaster... A well established and thoroughly tested disaster recovery plan must be developed in harmony with the BCM plan to increase the probability of successfully recovering vital organization records."²⁹

NIST, the purpose of BCP, "Provides procedures for sustaining mission/business operations while recovering from a significant disruption."³⁰

Effect: BC is instructions on how to work through a disaster; DR is instructions on how to recover from a disaster. The TS DRP/BCP has no distinction between activities that should be performed during a DRP versus a BCP; this lack of identifiable activities during a disaster will impact the effectiveness of the plans/actions resulting in poor utilization and allocation of resources, coordination and implementation of actions in a timely manner.

Many of the processes and procedures necessary to be performed during an incident may involve different tasks, depend on different suppliers or vendors, and/or have co-dependent activities. Technology components can require complex solutions, depending on their integrations, this could lead to gaps; therefore, it is important to have processes, procedures and responsibilities for DRP and BCP and their framework.



CONNECTION BETWEEN BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN ³¹

Cause: Combined DRP/BCP rather than independent plans with unique functions, activities, and requirements.

Recommendations:

- a. Create separate DRP and BCP processes, procedures, and responsibilities.

5. TS's DRP/BCP MANUAL LACKS FOUNDATIONAL CORE PRINCIPLES

Condition: The TS DRP/BCP manual does not disclose the basic core principles and/or fundamentals followed to create the department's manual.

Criteria: Best practices, most written DRP and BCP guides, policies, procedures, and standards notate and reference the governance/authority/principles the document is based on, aligned with, or follows. This is a common structural practice that enhances the credibility, reliability, and trustworthiness of the document's content.

Effect: The TS DRP/BCP document lists various requirements without stating the principals they are based on, referencing standards, applicable guidelines, or regulations:

- a) No fundamental principles and basis for its content.
- b) No provided references, acknowledgments, or credits for images used.

Example: Page 4 of the DRP/BCP manual displays an image of a triangle titled "Business continuity and disaster recovery planning" without references.

Not providing references and origin of content prevents the reviewer from authenticating the documents content and reliability.

It is frowned upon to take some else's work (i.e., ideas, images, etc.) without acknowledging and/or giving credit to the originating source.

Effective and acceptable DRP/BCP content contains and follows a set of steps that stemmed from verifiable, well established, and recognizable industry standards -known as best

practices-, governing entities (i.e. AZ Auditor, FEMA, etc.), or written departmental policies and procedures.


Example 1: Federal Emergency Management Agency (FEMA) Manual *-Pre-Disaster Recovery Planning Guide for Local Governments-* States where their guidance is from:

Federal Emergency Management Agency (FEMA): "The planning process introduced and discussed in this guide directly aligns with the process outlined in Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide 101 (CPG 101). This guide is formatted to follow the six steps of CPG 101 and presents six standard planning steps in Chapters 7 through 12 and then presents key recommended activities that are specific to pre-disaster recovery planning efforts. Figure 1 can help to serve as a basic orienting checklist for preparing for recovery."³²

Example 2: Arizona State Emergency Response and Recovery Plan.³³

Arizona State Emergency Response and Recovery Plan

The State of Arizona emergency management enterprise follows the 2016 Emergency Management Accreditation Program (EMAP) Standard to ensure a quality program. Arizona was first accredited in 2004, and was reaccredited in 2009, 2015, and 2020.



Cause: Management is not implementing or following best practices.

Recommendations:

Follow best practices:

- a. Update TS's DRP/BCP manual and provide the core founding principles of its content.
- b. Provide references and credit to content/images used in the TS DRP/BCP manual.

6. NO MANAGEMENT RESOLUTIONS TO THE FINDINGS OF THE NEW EXTERNAL TEST REPORT

CONDITION: The recently provided external test report, dated February 3, 2022, did not contain management's responses or scheduled corrections to the findings.

CRITERIA: Government Auditing Standards (GAO) – Requirement *-Results of Previous Engagements* – "6.11 - When planning the audit, auditors should ask management of the audited entity to identify previous audits, attestation engagements, and other studies that directly relate to the objectives of the audit, including whether related recommendations have been implemented. Auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that could have a significant effect on the subject matter. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current audit work and determining the extent to which testing the implementation of the corrective actions is applicable to the current audit objectives."³⁴

EFFECT: TS provided the External Test Report -performed by a third party on February 3, 2022- which listed several observations in need of improvement and correction; however, it did not include the department's Management Responses and Corrections (MRC's).

Responses to audit findings are an acknowledgment from management of the necessary corrections and a commitment to improve; they are necessary to perform required quality assurance of corrective actions.

NOTE: Recommendations for the findings in the external test report were in a confidential report; therefore, to preserve the confidentiality of the document, they will not be disclosed in this public report.

CAUSE: Management did not provide responses and/or commitments to the test findings.

RECOMMENDATION:

Address findings in a timely and acceptable manner.

Create a schedule for completion or measures that will be taken to mitigate the risks.

Provide MRC's or mitigating actions to the findings listed in the External Test Report.

7. UN-IMPLEMENTED MANAGEMENT RESPONSES AND CORRECTIONS (MRC'S) FROM CONSULTATION AUDIT

CONDITION: Specific to the previous Consultation Audit, some progress on the recommended and provided MRC's has been made.

CRITERIA: IIA -2500- Monitoring Progress – “The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

- 2500.A1- The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.
- 2500.C1- The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.”³⁵

IIA -2600- Communicating the acceptance of risks- “...If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.”³⁶

EFFECT: The consultation audit was performed to provide management with an opportunity to make improvements to DRP/BCP and its supporting documents. This Assurance Audit was scheduled during the exit meeting of the Consultation Audit; this provided management with a one-year opportunity to make corrections. The recently provided DRP/BCP manual and supplied information reflect some minor improvements (i.e., Business Continuity Plan was added to the manual's title, some of the oversights and missing data in the worksheets were corrected).

However, the TS DRP/BCP manual does not contain or provide sufficient guidance or steps for performing a recovery or for re-establishing continuity of operation(s). There are no adequate written procedures, structured processes, nor a supporting business impact analysis.

CAUSE: Unknown.

RECOMMENDATION:

Complete implementation of pending MRC's in a timely and acceptable manner.

Create and provide a schedule for estimated completion of open MRCs.

8. RESTRICTIONS AND DELAYED ACCESS TO INFORMATION

CONDITION: TS created delays on requested preliminary documents, requested extensions, re-schedules, and requested audit limitations.

CRITERIA: TUSD Policy-Code-DIFA -Office of Internal Audit (OIA) – Unrestricted Access: “The OIA shall be provided unrestricted access to all functions, records (including data and databases), property, and personnel relevant to the subject being reviewed... The OIA shall be free of interference in determining the scope of internal audits, performing audit work, and communicating audit results. Any auditee impositions, limitations, objections, and or issues, that could potentially impair or jeopardize the internal audit independence or the timely completion of an audit, shall be reported to the Superintendent or designee and/or the Governing Board and Audit Committee.”³⁷

EFFECT: The letter of intent to audit was sent to TS’s executive management and the Superintendent on June 21, 2022; it contained a list of preliminary items to be provided by June 28, 2022. A follow up e-mail from Internal Audit was sent inquiring about the pending documents on June 29, 2022; executive management responded on the same day and requested to re-schedule the audit to September or later. Internal audit was unable to grant the postponement given the short notice of the request. TS responded June 29, 2022, by requesting an additional ten business day extension to provide the requested preliminary documents and requested “...that no audit work is expected during the first two weeks of school in August.”

In response, Internal Audit agreed to eliminate a couple of meetings in order assist TS with their timeline, and to allow Internal Audit to adhere to the Audit Plan for SY: 2022-2023.

The compromise made with TS resulted in: Adjustments to the audit objectives, such as eliminating activities and responsibilities performed by vendors and employees, not testing, or verifying staff related DRP/BCP practices, procedures, and not attesting to DRP/BCP infrastructure and its location(s).

A stringent deadline due to the preliminary documents being provided ten business days late date, plus the request for ten business days of no audit work.

CAUSE: Inadequate planning and management of TS’s scheduled deadlines. This audit was scheduled to be conducted on the month previously selected by TS’s executive management.

RECOMMENDATION:

- a. Practice professional acumen: this requires re-scheduling or canceling appointment in advance.
- b. Manage and maintain proper recording of meetings and time management.

9. BUSINESS IMPACT ANALYSIS (BIA) REPORT

CONDITION: The provided BIA document contained limited information.

CRITERIA: According to TechTarget, “A business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. A BIA is an essential component of an organization's business continuity plan (BCP). It includes an exploratory component to

reveal any threats and vulnerabilities and a planning component to develop strategies for minimizing risk. The result is a business impact analysis report, which describes the potential risks specific to the organization studied. One of the basic assumptions behind a BIA is that every component of the organization relies on the continued functioning of all the others. However, some are more crucial than others and require a greater allocation of funds and operational resources in the event of a disaster.”³⁸

Global Technology Audit Guide (GTAG) -Business Continuity Management -5.3- Business Impact Analysis- “A BIA is used to identify critical business processes that need to be recovered following a disaster event....

A.- Identifying the Business Processes: The first step in a BIA is to identify the business processes performed by the functional team, the resources needed to perform the function, and the critical staff performing the work. The business processes initially should not be broken down into too many individual sub-processes. Business processes should be identified separately if they have different staffing (e.g., staff roles), service providers (e.g., third party, outsourcer, etc.), or resources (e.g., IT systems).

B.- Determining RTO and RPO Based on Business Impact: The second step in a BIA is to identify the type of business impact if the business process cannot be performed...Then, determine a recovery time objective (RTO) based on the types of business impact...Typically, the cost of the recovery solution will rise as the RTO decreases (i.e., if the business process must be restored immediately, the cost could be very high)...Next, determine a recovery point objective (RPO) for information systems. The RPO is the amount of data that can be lost if a disaster destroys the information systems...The Recovery Point Objective (RPO) is the amount a data that can be lost if a disaster destroys the information system...”³⁹

GTA’s image below illustrates an example of a Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

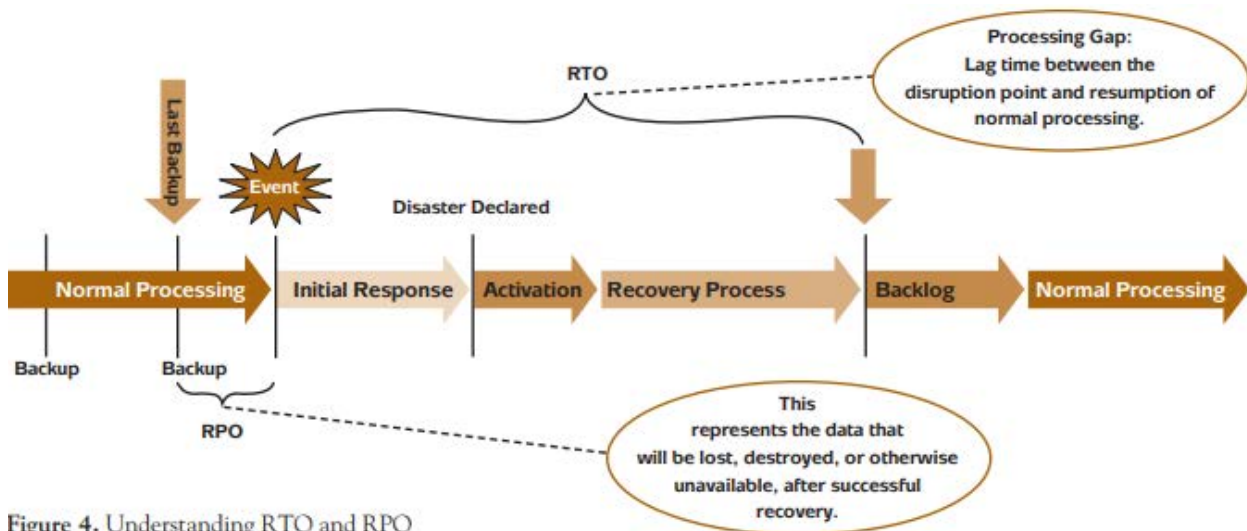


Figure 4. Understanding RTO and RPO

IMAGE RETRIEVED FROM GTAG 10: BUSINESS CONTINUITY MANAGEMENT⁴⁰

Ready, states that “A BIA report should document the potential impacts resulting from disruption of business functions and processes. Scenarios resulting in significant business

interruption should be assessed in terms of financial impact, if possible. These costs should be compared with the costs for possible recovery strategies.


The BIA report should prioritize the order of events for restoration of the business. Business processes with the greatest operational and financial impacts should be restored first."⁴¹

EFFECT: A BIA should identify key elements, essential processes, basic functions, and necessary resources for the business continuity plan at various levels of the organization.

The BIA document titled "Business Impact Analysis and Infrastructure Update Plan (BIA/IUP)" was provided in place of the requested BIA report. The document was dated "December 2021", the credited team was "TS Infrastructure and Architecture Teams"; it addressed "Upgrade Plan-Cloud Migration".

The document was segmented into four categories, structured in an outline format; it contained minimal information with no analysis of the impact -operational or financial- to the list of items, no measured timing, or duration of disruption. Example: (Image below)- Selected one out of the four items in the provided document by TS, titled "Business Impact Analysis and Infrastructure Upgrade Plan".

4. Recovery Systems and Resources



In order to preserve data integrity, reliability, proper backup and restoration, and in order to maintain continual business operations, it was determined to proceed with cloud migration to the Microsoft Azure platform for certain essential systems, in Spring and Summer 2022.

Subsequent migration may follow based on need, quality assurance, testing and performance in the cloud of the systems listed below and cost.

The list of systems included in the cloud migration in Spring & Summer 2022:

- 1) Active Directory (AD) and Azure Active Directory (AAD)
- 2) Library Management System (Destiny Web)
- 3) Printing Management and Audit System (Universal Printing System)
- 4) Some Business Intelligence Systems (BI)
- 5) Microsoft Identity Manager (MIM)
- 6) Some Data Backup Systems
- 7) Student Information System (SIS - Synergy)
- 8) Transportation System (Versatran)
- 9) TS Work Order Ticketing System (Trackit)

Technology Services

3






"BUSINESS IMPACT ANALYSIS AND INFRASTRUCTURE UPGRADE PLAN" by TS.⁴²

BIA reports are impact assessments that assist management in developing business continuity plans with identified activities to be prioritized, detected timing and duration of disruption, allocation of resources, and mitigation of risk.

TechTarget notes that “One of the basic assumptions behind a BIA is that every component of the organization relies on the continued functioning of all the others. However, some are more crucial than others and require a greater allocation of funds and operational resources in the event of a disaster.”⁴³

Example: (Image below)

Elements of business impact analysis

	Fire in data center	Loss of specialized staff	Vehicle crash in front entrance of office building	Vandalism to primary product assembly line	Loss of staff due to COVID-19 illness
BUSINESS ACTIVITY AFFECTED	All activities in data center	Activities that require specialized staff	All activities at that location unless an alternate access option is available	Loss of primary production line	Loss of possibly key employees needed to run the business
POTENTIAL OPERATIONAL LOSS	Inability to function normally	Reduced ability to function normally	Nominal disruption based on how quickly the vehicle can be removed and the front entrance reopened	Inability to produce the company's primary product	May be nominal to significant depending on who is affected
POTENTIAL FINANCIAL LOSS	\$3,000 to \$4,000 revenue loss per hour	None, assuming backup staff is available	None, assuming alternate entrance is available and access to building facilities is available	\$25,000 to \$40,000 per hour in lost revenue	Could be minimal assuming employees can work remotely
MINIMUM TIME NEEDED TO RECOVER OPERATIONS	Three to four hours	One to two hours	Depending on the damage from the crash, up to one day	Days if a work-around can be built; weeks if an alternate production facility must be found and launched	24-48 hours depending on health status and if employees can work remotely
					

ELEMENTS OF BUSINESS IMPACT ANALYSIS (BIA), by TechTarget⁴⁴

CAUSE: Not implementing the intended purpose and basic structure of a BIA report.

RECOMMENDATIONS:

- a. Identify and summarize anticipated impacts on the department's operations, such as:
 - Timing – The period in which an incident would have the most impact -e.g., Beginning of school year, end of the month, quarterly, etc.).
 - Duration – The length of interruption and restoration will vary depending on the analyzed event- (e.g., less than 1 hour, over 1 hour but less than 8 hours, etc.).
 - Operational Impact – Inability to perform activities or tasks created by the disruption that affected the department or programs, delays in operational system, data recovery, etc.

- Financial Impact – Additional cost due to damages resulting from the occurrence, such as, repairs or replacement of assets, data losses and recovery, etc.).
- b. Provided references for images used in the documents.

10. VAGUE DRP/BCP STANDARD OPERATING PROCEDURES

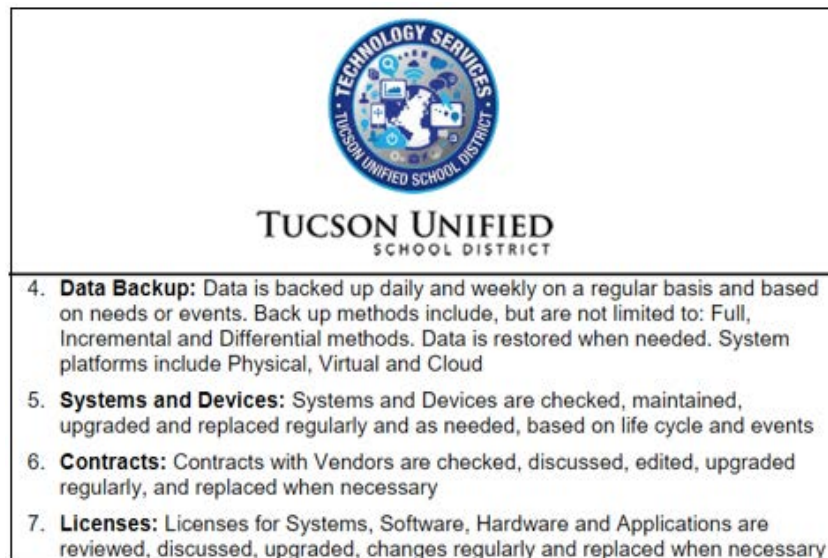
CONDITION: Standard Operating Procedures (SOP) for DRP/BCP do not provide sufficient guidance or instructions.

CRITERIA: Cybersecurity & Infrastructure Security Agency (CISA), "Standard Operating Procedures (SOPs) are formal, written guidelines or instructions for incident response that typically have both operational and technical components."⁴⁵

Tech Target defines SOPs as "A standard operating procedure is a set of written instructions that describes the step-by-step process that must be taken to properly perform a routine activity. SOPs should be followed the exact same way every time to guarantee that the organization remains consistent and in compliance with industry regulations and business standards. Standard operating procedures provide the policies, processes and standards needed for the organization to succeed. They can benefit a business by reducing errors, increasing efficiencies and profitability, creating a safe work environment and producing guidelines for how to resolve issues and overcome obstacles."⁴⁶

EFFECT: TS's Standard Operating Procedures do not contain sufficient instructions to properly conduct the activities listed in the document.

EXAMPLE: (Image below -Page 2/2) Excerpt from TS provided document, titled "Standard Operating Procedures for Disaster Recovery & Business Continuity"



"STANDARD OPERATING PROCEDURES FOR DISASTER RECOVERY & BUSINESS CONTINUITY" by TS⁴⁷

CAUSE: The document has not been created or updated appropriately.

RECOMMENDATIONS:

Follow best practices when developing SOP's.

11. VARIATIONS BETWEEN DEVICES LISTED IN THE SUPPORTING DATA AND TS’S DRP/BCP MANUAL

CONDITION: Some devices listed in the TS DRP/BCP manual -Section VIII -Network Infrastructure were not included in the supporting data.

CRITERIA: Best practices, maintain accurate records of equipment and systems; ensure changes and updates are coordinated and reflected in the department’s reference and supporting materials.

EFFECT: The TS DRP/BCP manual is a reference material that should contain accurate and reliable information. Discrepancies between reference material and supporting documents render both documents unreliable.

TS’s DRP/BCP manual -Section VIII- “Network Infrastructure Failover Procedures – listed several devices that were not listed and/or were removed in the provided supporting document titled “4.Audit-TS-DRBC-1-DRBCDeviceList-July.12.22- Tab: “NETWORK DATA“ (Worksheet) -Modified image of the Worksheet below:

TYPE	TIER (0-3)	OWNER	STAKEHOLDERS	BUSINESS PROCESSDEPENDENCIES	BACKUP/RESTORE PROCESS	ACTIVE - Y/N	NOTES
Physical	0	[Redacted]	[Redacted]	[Redacted]	Vendor Coverage	N	Removed
Physical	0				Vendor Coverage	N	Replaced wi
Physical	0				Vendor Coverage	Y	Added summer
Physical	0				Vendor Coverage	Y	Added summ
Physical	0				Vendor Coverage	N	To be removed
Physical	0				Vendor Coverage	N	To be removed
Physical	0				Vendor Coverage	Y	
Physical	0				Vendor Coverage	Y	
Physical	0				Vendor Coverage	Y	
Physical	0				Vendor Coverage	Y	
Physical	0				Vendor Coverage	Y	
Physical	0				Vendor Coverage	N	To be removed
Physical	0				Vendor Coverage	N	To be removed
Physical	0				Vendor Coverage	N	To be removed
Physical	0				Vendor Coverage	N	To be removec

“4.AUDIT-TS-DRBC-1-DRBCDEVICELIST-JULY.12.22- TAB: “NETWORK DATA“⁴⁸

The total number of items found in the provided Worksheet that differed from the Section VIII of the DRP/BCP are summed in the table below.

# Missing/ Total Items	System Name	Owners	Stakeholder	Business Process /Dependencies	Backup/Restore Process
2/7	[Redacted]	TS Network Team	District-Wide	All District’s Network Access	Vendor Coverage
2/14					
11/91					

CAUSE: Lack of coordination between documents.

RECOMMENDATIONS:

Create and follow procedures the reduce the risk of conflicting or contradictory information.

12. RESULTS IN TS’S BACKUP LOG

Condition: No explanation of, or corrections for, failed jobs and failed objectives in the provided “BackupLog-Physical Virtual2-July2022”.

Criteria: Best practices, when providing documents to an auditor that contain “Failed” actions it is recommended to include reasons and/or the intended corrections.

Effect: Provided “BackupLog-Physical Virtual2-July2022” (Image below), contained errors and failures with the reason for the error, but do not indicate if they were corrected.

Summary						
Job status	Total Jobs	Size of Application	Media Size	Protected Objects	Failed Objects	Failed Folders
Completed					2	0
Completed with errors					80	0
Failed					0	0

TS’S PROVIDED -SUMMARY- “BACKUPLLOG-PHYSICAL VIRTUAL2-JULY2022”⁴⁹

Cause: Management did not review the submitted summary and submitted it without properly addressing the “Completed with errors” and “Failed” statuses.

Recommendations:

Preemptively address failed items and include upcoming corrections and/or pending implementations with estimated completion dates.

13. OVERSIGHTS IN TS’S DRP MANUAL

Condition: The DRP Manual for the IT Department contains several changes, undisclosed references, and oversights.

Criteria: Best practices, regardless of the industry, written material should be verified and reviewed, prior to distribution, to ensure content is accurate, contains applicable references, and is free of spelling and grammatical errors.

Effect: Reliability of content material is diminished by undisclosed references and errors. Over thirty oversights were detected on the TS DRP/BCP document; a selected few are listed below:

- Index numbers and content do not match and are out of order; the index shows 13 pages, but the document contains 19 pages.
- No reference to original creator of Figure 1 –“Disaster Recovery and Business Continuity Areas and Processes.”
- Change in District Operations Checklist, the Chief Technology Officer was removed from the list.
- Change Section III – Disaster Event Declaration- “...individual acting in CTO capacity” was removed.
- Section IX. Applications Replication and Failover Strategy (B). Applications Failover Conditions and Requirements –“This district’s critical systems...attached *DRBC Device List* for Systems and Applications Tiers classifications and Essential Information.” There was no attachment or Appendix disclosing an attachment.

Cause: Oversight on the TS’s DRP/BCP document.

Recommendations:

Review the TS’s DRP/BCP and correct the material prior to distribution.

CONCLUSION

This compliance audit was performed on the TS DRP/BCP; its purpose was to determine the plan's effectiveness, efficiencies, compliance, and readiness to address a disaster, prior, during, and after it occurs. This audit utilized some of the information provided during the consultation audit of TS DRBCP, completed on June 30, 2021 to assess the updated TS DRP/BCP data.

The Institute of Internal Audit (IIA) classifies audits as either assurance or consultations. The main difference between them is their level of risk, management's involvement during the audit process, and report distribution.

This audit was conducted a year after the consultation audit; the time laps between the two audits was to allow management an opportunity to implement their provided MRCs in the consultation report.

The focus of this audit was to review TS's processes and procedures regarding DRP/BCP. The current TS management and staff have proven and demonstrated their capable while effectively navigating the District through the most resent pandemic.

It is Internal Audit's opinion that, while TS has made some progress on their DRP/BCP, there is room for improvement.

The department does not have applicable written DRP/BCP policies, specific procedures, and detailed guidelines to ensure operating activities would be restored and re-established. Its current DRP/BCP and related documents would not effectively prepare or ensure essential operations could/would re-establish "business as usual" operations after a disaster. The objectives for this audit were designed to determine areas in need of improvement, they were similar to the objectives from the consultation audit. However, due to the time constraints, vendor verification and employee related activities were excluded from this audit.

The objectives were achieved by analyzing and reviewing the provided data from TS, by assessing the previous audit questionnaire, and comparing existing information to acceptable standards, guidelines, and district polices.

Provided audit recommendations are based on TS's DRP/BCP documents against reviewed DRP and BCP fundamental standards, DRP/BCP policies, procedures, and detailed research of leading organizations' best practices and governing agencies.

Audit findings were addressed with TS's Interim Executive Director on August 17, 2022.

A draft copy of this report was provided to TS Executive Management, Audit Committee, Legal Counsel, Superintendent, and staff, for their review and impute on August 18, 2022.

A follow up audit of the TS DRP/BCP will be conducted in approximately fifteen months (currently estimated to be November 2023) from the date this final report is delivered to the Governing Board. The follow up audit will focus on verify the implementations of the MRCs listed in this final audit report.

ACKNOWLEDGMENT

The Office of Internal Audit wishes to express its appreciation to the TS department and staff for their time in providing the requested preliminary documentation for this assurance audit.

Martha Smith 8/31/2022
Martha Smith Date
Internal Auditor

Report Distributed:

Honorable Chairwoman and
Members of the Governing Board:

Adelita Grijalva, President
Natalie Luna Rose, Clerk
Sadie Shaw
Leila Counts
Dr. Ravi Grivois

Superintendent and Management:

Dr. Gabriel Trujillo, Superintendent
Robert Ross, Legal Counsel
Blaine Young, Chief Operating Officer
Rabih Hamadeh, Interim Executive Director

Audit Committee Chair and Members:

Dr. William Kelly, Chair
Bernie Wiegandt, Vice-Chair
Natalie Luna Rose, Board Clerk and Committee Ex-Officio

Sarina Martinez
Jodi Perin

TUCSON UNIFIED
SCHOOL DISTRICT
Technology Services
October 2019

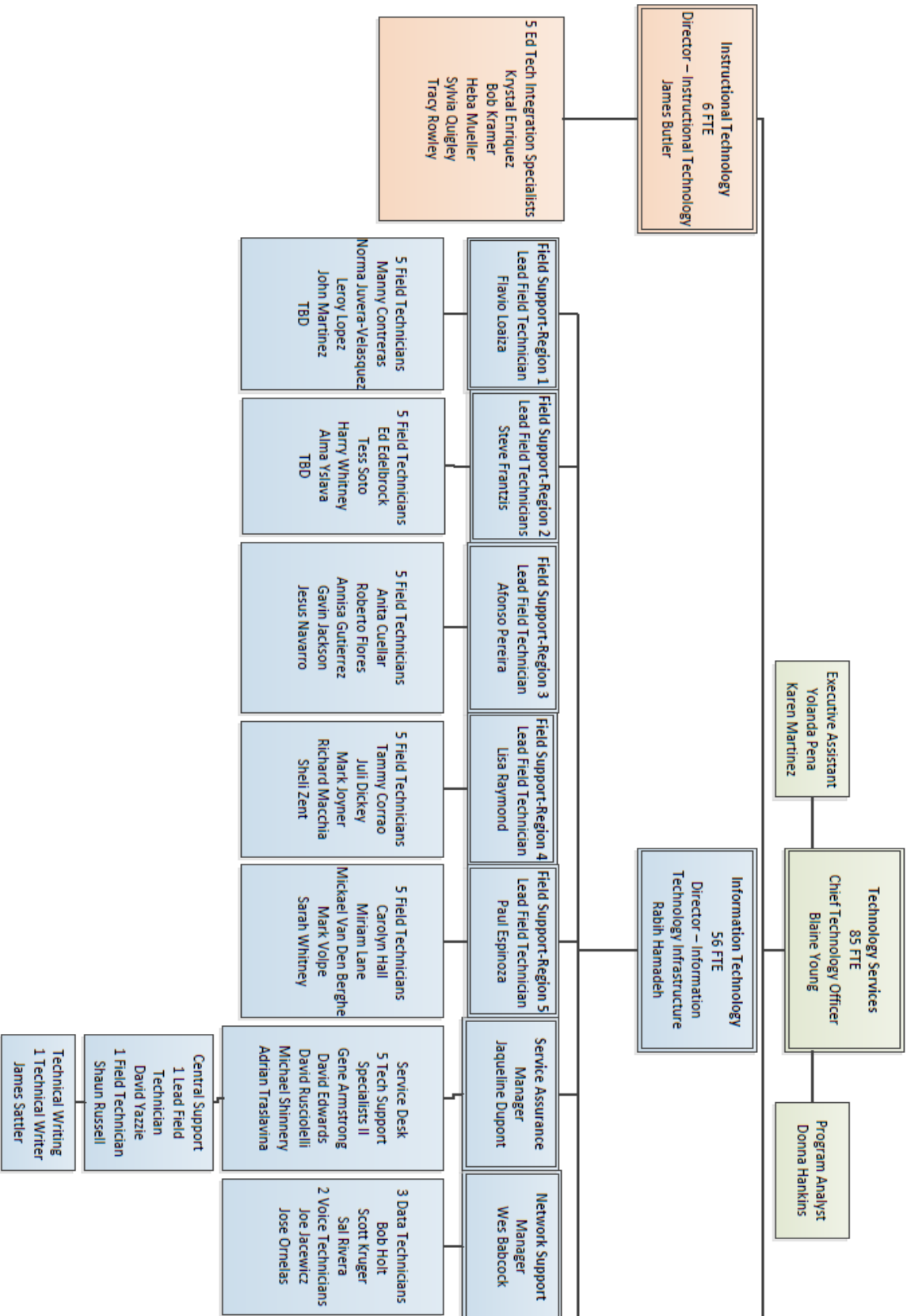


FIGURE 1

Continuation of Organizational Chart for
Technology Services

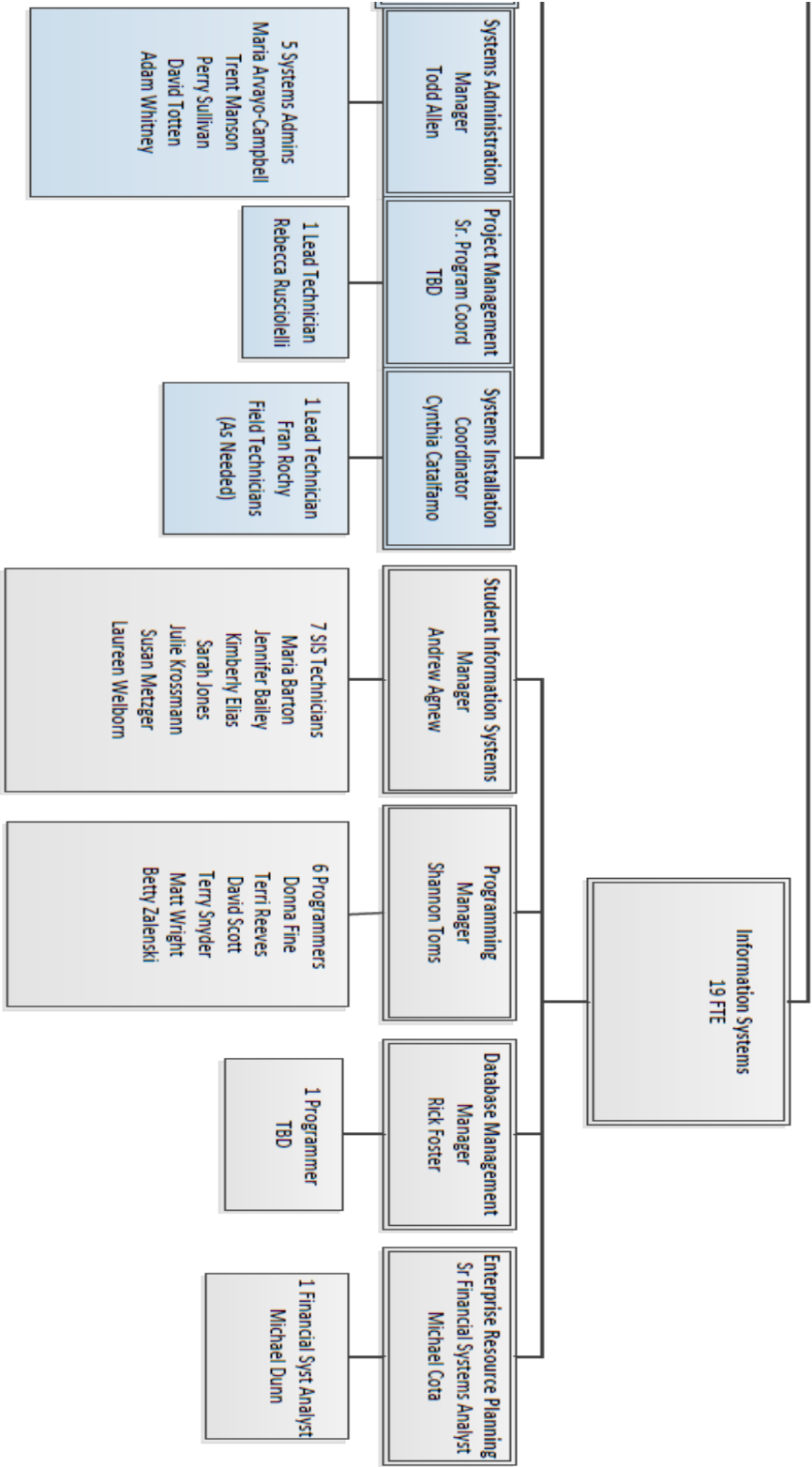


FIGURE 2

REFERENCES

1. **TS Department** - “The Tucson Unified School District's Technology Services Department is committed to enhancing and improving the District's technology resources and support at all of the District’s schools on an equitable basis. The data network we support extends over 250 square miles and serves approximately 43,000 students and 8,300 staff. Our network is one of the largest in the state!” <http://www.tusd1.org/Departments/Technology-Services>
2. **Policy Code A: Foundation and Basic Commitments:** “The Districts’ mission, in partnership with parents and the grater community, is to assure each pre-K through 12th grade student receives an engaging, rigorous and comprehensive education. The District is committed to inclusion and non-discrimination in all District activities.” (July 13, 2018), <http://govboard.tusd1.org/Policies-and-Regulations/Policy-Code-A>
3. **The Institute of Internal Auditors (IIA):** Definition- Assurance Audits – “An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.” <https://global.theiia.org>
4. **IIA:** Definition- Consultation Audits- “Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization’s governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, ad training.” (2022); <https://global.theiia.org>
5. **Arizona Auditor General (AZ Auditor)** – Image- of “Risk and Business Contingency Planning”, (Pager 4), from power point presentation given on June 22, 2016 by Jennie Snedecor and Katie Morris. (2018) https://www.azauditor.gov/sites/default/files/Contingency%20Planning_2.pdf
6. **Information Systems Audit and Control Association (ISACA):** Glossary –“DR- Disaster Recovery: Activities and programs designed to return the enterprise to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan (DRP) to restore an enterprise's critical business functions.” (2018) <https://www.isaca.org/resources/glossary#glossd>
7. **ISACA:** Glossary-BCP- “Business Continuity Plan: A plan used by an enterprise to respond to disruption of critical business processes. An organization depends on the contingency plan for restoration of critical systems.” <https://www.isaca.org/resources/glossary#glossd>
8. **ISACA** -Auditing BCM Pondurance ISACA Presentation: Image of “Business Continuity Management (BCM) – An Auditor’s Perspective, by Kathy Pelletier on 6/26/15. <https://www.isaca.org/resources>
9. **The National Institute of Standards and Technology (NIST):** 2.2.6 *Disaster Recovery Plan (DRP)* - Definition of the DRP- “A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. The DRP may be supported by multiple information

system contingency plans to address recovery of impacted individual systems once the alternate facility has been established. A DRP may support a BCP or COOP plan by recovering supporting systems for mission/business processes or mission essential functions at an alternate location. The DRP only addresses information system disruptions that require relocation.” <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>

10. **NIST –2.2.1 Business Continuity Plan BCP-** “The BCP focuses on sustaining an organization’s mission/business processes during and after a disruption. An example of a mission/business process may be an organization’s payroll process or customer service process. A BCP may be written for mission/business processes within a single business unit or may address the entire organization’s processes. The BCP may also be scoped to address only the functions deemed to be priorities. A BCP may be used for long-term recovery in conjunction with the COOP plan, allowing for additional functions to come online as resources or time allow. Because mission/business processes use information systems (ISs), the business continuity planner must coordinate with information system owners to ensure that the BCP expectations and IS capabilities are matched.” <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>
11. **TechTarget,** “Disaster recovery (DR) and business continuity planning are often linked, but they are different. A DR plan is reactive, as it details how an organization recovers after a business disruption. A business continuity plan is a proactive approach that describes how an organization can maintain business operations during an emergency.” May 2022, by Vicki-Lynn Brunskill, <https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity-action-plan>
12. **AZ Auditor – Image of “Risk and Business Contingency Planning”,** (Pager 11), from power point presentation. June 22, 2016, by Jennie Snedecor and Katie Morris; https://www.azauditor.gov/sites/default/files/Contingency%20Planning_2.pdf
13. **AZ Auditor -** “The items necessary for each plan may vary by entity, but some basic DRP components include the following:
 - Identification of critical equipment, data, and resources, including off-site locations to store backup data and maintain redundant system resources to allow for emergency data processing.
 - Contact list of key individuals including their roles and responsibilities. Procedures for regularly backing up systems and data, and regularly testing backups.
 - Procedures for activating the DRP, notifying appropriate parties, and assessing the severity of the disruption and the required response.
 - Steps and procedures for restoring systems to full functionality.
 - Supporting information as necessary to ensure a comprehensive plan such as business impact analysis, vendor contact information, etc.” <https://www.azauditor.gov/reports-publications/school-districts/faqs/information-technology>
14. **Internal Audit Questionnaire - (5/6/21) TS DRDRP Consultation Audit in Team SharePoint.** LEDGEN: Original questions are in black font. Management’s 1st set of answers are in BLUE

font. Clarification questions are in RED font. Management’s 2nd set of answers are highlighted in GRAY. 2nd Clarification questions from auditor are in GREEN font. Management 33rds set of answers are highlighted in green.

Section: POLICY
 1. Does IT have departmental written policies for DRP? DR/BC Processes part of DRP – revised January 2021—Please clarify, is IT classifying the DR document as the policy? Please clarify, is IT classifying the DR document as the policy? Yes. District Policy formulation update in progress. Ok, so as of today, there is no DR policy in place. In other words, it is not in the Governing Boards site where anyone can read it, correct? Correct

15. **The Arizona State Emergency Response and Recovery Plan (SERRP)** “Is an all-hazards plan addressing Arizona’s hazard and threat environment, including natural, technological, and human caused emergencies or disasters. The SERRP is written to support the Arizona Department of Emergency and Military Affairs, Emergency Management (DEMA-EM) mission to provide emergency management capabilities to the citizens of Arizona and the Nation.

The plan is designed as a high tier Whole Community document identifying state agency roles and responsibilities during an emergency or disaster. TPg. BP-1; November 2018 - https://dema.az.gov/sites/default/files/publications/EM-PLN_SERRP.pdf

16. **NIST - Special Publication 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems**, provides instructions, recommendations, and considerations for federal information system contingency planning. Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.”
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>

17. **NIST – Image: NIST’s image from the partial Table of Contents of The National Institute of Standards and Technology (NIST) Special Publication 800-184**, shows some of common items in a DRP guide. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf>

18. **ISACA Journal - IS Audit Basics: Backup and Recovery-**(January 1, 2018), “Create a Recovery Team with Roles and Responsibilities – The team should include all the functions and roles necessary to quickly and completely restore computer operations. There should be a document that identifies the team members, their respective roles and the steps each would take in restoring operations.” https://www.isacajournal-digital.org/isacajournal/2018_volume_1/MobilePagedArticle.action?articleId=1281345#articleId1281345

19. **AZ Auditor – Frequently Asked Questions #6-** “The items necessary for each plan may vary by entity, but some basic DRP components include the following:
 - Identification of critical equipment, data, and resources, including off-site locations to store backup data and maintain redundant system resources to allow for emergency data processing.
 - Contact list of key individuals including their roles and responsibilities.

- Procedures for regularly backing up systems and data, and regularly testing backups.
 - Procedures for activating the DRP, notifying appropriate parties, and assessing the severity of the disruption and the required response.
 - Steps and procedures for restoring systems to full functionality.
 - Supporting information as necessary to ensure a comprehensive plan such as business impact analysis, vendor contract information, etc.” <https://www.azauditor.gov/reports-publications/school-districts/faqs/information-technology>
20. **TS DRP/BCP Manual** – Image- Table of Content, July 2022, SharePoint Folder.
 21. **AZed** - quoted “The National Incident Management System (NIMS) defines preparedness as “a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response.” The Preparedness Cycle was created to illustrate the following steps: Plan, Organize/Equip, Train, Exercise, Evaluate/Improve. Each stage in the Preparedness Cycle relates to one or more of the five mission areas in the National Preparedness Goal, as outlined by the U.S. Department of Homeland Security (2015).” <https://www.azed.gov/wellness/sep>
 22. **AZed** -Image of “The Preparedness Cycle by AZed. <https://www.azed.gov/wellness/sep>
 23. **AZ Auditor** –Image- Call Tree from the *Risk and Business Contingency Planning: Developing a Contingency Plan Activation and Notification-* Slide, (Page 26)- Power point presentation, 6/22/2016, State of Arizona Office of the Auditor General, by Jennie Snedecor and Katie Morris. https://www.azauditor.gov/sites/default/files/Contingency%20Planning_2.pdf
 24. **TS DRP/BCP Manual** – “The DR & BC team member who dials in first will setup an instant meeting room via the portal.” Page 10, July 2022, SharePoint Folder.
 25. **ISACA Journal Archives** –*What Every IT Auditor Should Know About Backup and Recovery-* November 1, 2011 - “These manuals are needed because members of the recovery team may not normally do some of the business processes.” <https://www.isaca.org/resources/isaca-journal/past-issues/2011/what-every-it-auditor-should-know-about-backup-and-recovery>
 26. **AZed** - “Arizona School Emergency Operations Plans (EOP)- (EOP Minimum Requirements - Arizona Revised Statutes (ARS) 15-341 (A) (31)- A variety of resources that include guides, training materials and technical assistance are available to schools relative to the process of revising or developing a comprehensive emergency operations plan that meets the individual needs of the school. ADE, AZDEMA, Department of Health Services (AZDHS), and the Arizona Department of Public Safety (AZDPS) recognizes a national 6-step process of plan development, as outlined in the two aforementioned national resource documents. Image/Figure 1 depicts the six steps in the planning process. Each step in the planning process, Schools should consider the impact of their decisions on ongoing activities such as training and exercises, as well as on equipment and resources” Arizona Department of Education, April 2019; <https://www.azed.gov/sites/default/files/2019/08/AZ%20School%20EOP%20Minimum%20Requirements%20-%20FINAL.pdf?id=5d54571e1dcb250abc4a8245>

27. **AZed –Image-** Arizona School Emergency Operation Plans (EOP).
<https://www.azed.gov/sites/default/files/2019/08/AZ%20School%20EOP%20Minimum%20Requirements%20-%20FINAL.pdf?id=5d54571e1dcb250abc4a8245>
28. **TS DRP/BCP Manual -Section III. Disaster Event Declaration-** (Page 6) - “Impacts and related actions resulting from an existing district extend well beyond the needs and actions of the IT team and IT systems. Actions could include providing temporary workspace, relocating key employees and initiating emergency evacuation procedures. These actions and the TS DRP & BCP are part of a larger District-wide DRP & BCP.” July 2022, Microsoft Team Folder.
29. **Global Technology Audit Guide (GTAG) -Business Continuity Management –** (Page 3) - 2.3 Disaster Recovery of IT, states “Disaster... A well established and thoroughly tested disaster recovery plan must be developed in harmony with the BCM plan to increase the probability of successfully recovering vital organization records.”
https://www.iaa.nl/SiteFiles/IIA_leden/Praktijkgidsen/GTAG10.pdf
30. **NIST-** the purpose of BCP, “Provides procedures for sustaining mission/business operations while recovering from a significant disruption.”
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.p>
31. **Premathas Somasekarm -Image-** Connection between business continuity plan and disaster recovery plan- Uppsala Universitet -A Component-based Business Continuity and Disaster Recovery Framework- March 22017. <https://www.diva-portal.org/smash/get/diva2:1108197/FULLTEXT01.pdf>
32. **FEMA-**“Federal Emergency Management Agency (FEMA): “The planning process introduced and discussed in this guide directly aligns with the process outlined in Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide 101 (CPG 101). This guide is formatted to follow the six steps of CPG 101 and presents six standard planning steps in Chapters 7 through 12 and then presents key recommended activities that are specific to pre-disaster recovery planning efforts. Figure 1 can help to serve as a basic orienting checklist for preparing for recovery.”” September 2021, Version 3.0; https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf
33. **Arizona State Emergency Response and Recovery Plan -Image-** Acknowledgment of principles being followed. - https://dema.az.gov/sites/default/files/publications/EM-PLN_SERRP.pdf
34. **Government Auditing Standards (GAO) – Requirement -Results of Previous Engagements –** “6.11 - When planning the audit, auditors should ask management of the audited entity to identify previous audits, attestation engagements, and other studies that directly relate to the objectives of the audit, including whether related recommendations have been implemented. Auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that could have a significant effect on the subject matter. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current audit work and determining the extent to which testing the implementation of the corrective actions is applicable to the current audit objectives.” Revised 2021, Page 129, <https://www.gao.gov/assets/720/713761.pdf>

35. **IIA -2500- MONITORING PROGRESS** – “The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.
- 2500.A1- The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.
 - 2500.C1- The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.”
<https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/standards/performance-standards/>
36. **IIA -2600- Communicating the acceptance of risks**- “...If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.” <https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/standards/performance-standards/>
37. **TUSD Policy-Code-DIFA -Office of Internal Audit (OIA) – Unrestricted Access**: “The OIA shall be provided unrestricted access to all functions, records (including data and databases), property, and personnel relevant to the subject being reviewed... The OIA shall be free of interference in determining the scope of internal audits, performing audit work, and communicating audit results. Any auditee impositions, limitations, objections, and or issues, that could potentially impair or jeopardize the internal audit independence or the timely completion of an audit, shall be reported to the Superintendent or designee and/or the Governing Board and Audit Committee.” <https://govboard.tusd1.org/Policies-and-Regulations/Policy-Code-DIFA>
38. **TechTarget** - “A business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. A BIA is an essential component of an organization's business continuity plan (BCP). It includes an exploratory component to reveal any threats and vulnerabilities and a planning component to develop strategies for minimizing risk. The result is a business impact analysis report, which describes the potential risks specific to the organization studied. One of the basic assumptions behind a BIA is that every component of the organization relies on the continued functioning of all the others. However, some are more crucial than others and require a greater allocation of funds and operational resources in the event of a disaster.”
<https://www.techtarget.com/searchstorage/definition/business-impact-analysis>
39. **GTAG – Business Continuity Management -5.3- Business Impact Analysis**- “A BIA is used to identify critical business processes that need to be recovered following a disaster event. The BIA may include an initial discussion of recovery solutions needed to resume the critical business processes (see “Business Recovery and Continuity Strategy” on page 11). Participants in the BIA should include staff from the business as well as key suppliers. The BIA should be performed with the knowledge from the BC risk assessment that defined the

credible events that could disrupt the business. Typically, BIA meetings are performed individually for each team. Then, discussions occur with the other teams identified as critical providers after each BIA meeting.

A. Identifying the Business Processes The first step in a BIA is to identify the business processes performed by the functional team, the resources needed to perform the function, and the critical staff performing the work. The business processes initially should not be broken down into too many individual sub-processes. Business processes should be identified separately if they have different staffing (e.g., staff roles), service providers (e.g., third party, outsourcer, etc.), or resources (e.g., IT systems).

B. Determining RTO and RPO Based on Business Impact The second step in a BIA is to identify the type of business impact if the business process cannot be performed. Below are some types of business impacts: • Health and safety (e.g., injury). • Environmental (e.g., spill). • Customer service (e.g., loss of customers). • Financial (e.g., penalties). • Regulatory/legal (e.g., governmental action). • Reputation (e.g., loss of image).

Then, determine a recovery time objective (RTO) based on the types of business impact. An RTO is a duration of time and service level within which a business process must be restored (after a disaster) to avoid unacceptable consequences associated with a disruption in continuity. An RTO is typically identified based on standard time markers of 0, 3, 7, 14, or 30 days. The business management ultimately determines the correct RTO for each business process. Typically, the cost of the recovery solution will rise as the RTO decreases (i.e., if the business process must be restored immediately, the cost could be very high).

Next, determine a recovery point objective (RPO) for information systems. The RPO is the amount of data that can be lost if a disaster destroys the information systems. Business staff must determine how many days' worth of data can reasonably be lost and recreated manually. Data can often be recreated from other sources such as external systems that exchange data with the organization system (e.g., banking systems). The business management ultimately determines the correct RPO for each business process. Typically, the cost of the recovery solution will rise as the RPO decreases (i.e., if the business process cannot afford to lose any data, the cost of data replication could be very expensive).” <https://www.iicolombia.com/resource/guias/GTAG10.pdf>

40. **GTAG -Image-** Business Continuity Management for Identifying the business process. Pg. 10, July 2008; https://www.ii.nl/SiteFiles/IIA_Jeden/Praktijkgidsen/GTAG10.pdf
41. **Ready** - “A BIA report should document the potential impacts resulting from disruption of business functions and processes. Scenarios resulting in significant business interruption should be assessed in terms of financial impact, if possible. These costs should be compared with the costs for possible recovery strategies.

The BIA report should prioritize the order of events for restoration of the business. Business processes with the greatest operational and financial impacts should be restored first.” <https://www.ready.gov/business-impact-analysis>

42. **TS's -Image** – “Business Impact Analysis and Infrastructure Upgrade Plan”. Page 3 Microsoft Team Folder.
43. **Tech Target** –“One of the basic assumptions behind a BIA is that every component of the organization relies on the continued functioning of all the others. However, some are more crucial than others and require a greater allocation of funds and operational resources in the event of a disaster.). By Paul Kirvan and Carol Sliwa. Tech Target: 2000-2022. <https://www.techtarget.com/searchstorage/definition/business-impact-analysis>
44. **Tech Target -Image- Elements of Business Impact Analysis (BIA)**. By Paul Kirvan and Carol Sliwa. Tech Target: 2000-2022. <https://www.techtarget.com/searchstorage/definition/business-impact-analysis>
45. **”Cybersecurity & Infrastructure Security Agency (CISA) - "Standard Operating Procedures (SOPs) are formal, written guidelines or instructions for incident response that typically have both operational and technical components.** <HTTPS://WWW.CISA.GOV/SAFECOM/SOPS>
46. **TechTarget – Standard Operating Procedures (SOP)-** “A standard operating procedure is a set of written instructions that describes the step-by-step process that must be taken to properly perform a routine activity. SOPs should be followed the exact same way every time to guarantee that the organization remains consistent and in compliance with industry regulations and business standards. Standard operating procedures provide the policies, processes and standards needed for the organization to succeed. They can benefit a business by reducing errors, increasing efficiencies and profitability, creating a safe work environment and producing guidelines for how to resolve issues and overcome obstacles. Kate Brush, October 2021, <https://www.techtarget.com/searchbusinessanalytics/definition/standard-operating-procedure-SOP>
47. **TS DRP/BCP SOPs – Image- “Standard Operating Procedures for Disaster Recovery & Business Continuity”.** Page 2 – Microsoft Team Folder.
48. **TS -Image-** of provided document titled “4.AUDIT-TS-DRBC-1-DRBCDEVICELIST-JULY.12.22- TAB: “NETWORK DATA“ Microsoft Team Folder.
49. **TS -Image-** Summary of “BackupLog-Physical Virtual2-July2022” . Microsoft Team Folder.
50. **Stock Adobe -Image** – Cover Page of Internal Audit Report for TS DRP/BCP Report. https://stock.adobe.com/sk/search/images?filters%5Bcontent_type%3Aphoto%5D=1&filters%5Bcontent_type%3Aillustration%5D=1&filters%5Bcontent_type%3Azip_vector%5D=1&filters%5Bcontent_type%3Avideo%5D=0&filters%5Bcontent_type%3Atemplate%5D=0&filters%5Bcontent_type%3Ad%5D=0&filters%5Bcontent_type%3Aaudio%5D=0&filters%5Binlude_stock_enterprise%5D=0&filters%5Bis_editorial%5D=0&filters%5Bfree_collection%5D=0&filters%5Bcontent_type%3Aimage%5D=1&order=relevance&price%5B%24%5D=1&safe_search=1&limit=100&search_page=1&search_type=see-more&serie_id=301917265&get_facets=0&asset_id=251060529

GLOSSARY

American Institute of Certified Public Accountants (IACPA): “Is the national professional organization of Certified Public Accountants in the United States, with more than 418,000 members in 143 countries in business and industry, public practice, government, education, student affiliates and international associates.” <https://www.aicpa.org/>

Arizona Auditor General (AZ Auditor) - The Arizona Auditor General serves as an independent source of impartial information concerning State and local governmental entities and provides specific recommendations to improve the operations of those entities”
<https://www.azauditor.gov/office-overview>

Arizona Strategic Enterprise Technology (ASET) - In alignment with the strategic missions of state agencies, ADOA-ASET develops and executes the statewide information technology strategy, as well as provides capabilities, services and infrastructure to ensure the continuity of mission critical and essential systems for the State of Arizona” <https://aset.az.gov/about>

Assurance audit – “The motive of assurance is not to correct the issues in accounting records but to measure the appropriateness as per accounting standards, principles and follow it's compliance. Moreover, assurance is applied to other aspects such as to assess the procedures and processes followed in operations. In such a case, processes and operations are closely observed and assurance will be provided whether the process is being conducted on the basis of the specified procedure to obtain optimum results.” <http://educba.com>

Best Practice - “A procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption.” Defined by Merriam Webster

COBIT: Control Objectives for Information and Related Technology -It is a framework created by the ISACA (Information Systems Audit and Control Association). It was designed to be a supportive tool for managers—and allows bridging the crucial gap between technical issues, business risks, and control requirements.” <https://www.isaca.org/resources/cobit>

Continuity of Operations Plan (COOP) - A predetermined set of instructions or procedures that describe how an organization’s mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.
https://csrc.nist.gov/glossary/term/continuity_of_operations_plan

Contract - Defined by Arizona state legislature: “means all types of state agreements, regardless of what they may be called, for the procurement of materials, services, construction, construction services or the disposal of materials.” <https://www.azleg.gov/ars/41/02503.htm>

Control - The Institute of Internal Auditors (IIA) defines control as any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goal will be achieved.
https://csrc.nist.gov/glossary/term/continuity_of_operations_plan

Disaster Recovery Plan – A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
https://csrc.nist.gov/glossary/term/disaster_recovery_plan

International Electrotechnical Commission (IEC) – Founded in 19060, the IEC is the world’s leading organization for the preparation and publication of international standards for all electrical electronic, electronica and related technologies. These are known collectively as “electrotechnology”. <https://www.iec.ch/who-we-are>

General Accepted Auditing Standards (GAAS): Are sets of standards against which the quality of audits are performed and may be judged. Several organizations have developed such sets of principles, which vary by territory. <https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00150.pdf>

Generally Accepted Government Auditing Standards (GAGAS): Also known as the Yellow Book, are the guidelines for audits created by the Comptroller General and the audit agency of the United States Congress, the Government Accountability Office. <https://www.gao.gov/yellowbook/overview>

Federal Information System Controls Audit Manual (FISCAM). “The FISCAM presents a methodology for performing information system (IS) control audits of federal and other governmental entities in accordance with professional standards, and was originally issued in January 1999.” “The FISCAM provides a methodology for performing information system (IS) control audits in accordance with GAGAS, where IS controls are significant to the audit objectives.” <https://www.gao.gov/assets/gao-09-232g.pdf>

Global Technology Audit Guide (GTAG) - Prepared by the IIA, each Global Technology Audit Guide (GTAG) is written in straightforward business language to address timely issues related to information technology (IT) management, risk, control, and security. The GTAG series serves as a resource for chief audit executives on different technology-associated risks and recommended practices. [https://na.theiia.org/standards-guidance/topics/pages/information-technology.aspx#:~:text=Global%20Technology%20Audit%20Guides%20\(GTAG%C2%AE\)&text=The%20GTAG%20series%20series%20as,GTAGs%20from%20the%20IIA%20Bookstore](https://na.theiia.org/standards-guidance/topics/pages/information-technology.aspx#:~:text=Global%20Technology%20Audit%20Guides%20(GTAG%C2%AE)&text=The%20GTAG%20series%20series%20as,GTAGs%20from%20the%20IIA%20Bookstore).

Industry Standard – “Is the average by which those in a particular field govern themselves. It is the ordinary manner of doing things in that field and can serve to establish different things in various legal settings.” Defined by HG Legal Resources <https://www.hg.org/legal-articles/what-is-the-relevance-of-industry-standards-under-the-law-36794>

Information Systems Auditor and Control Association (ISACA) – “ISACA stands for Information Systems Audit and Control Association. It develops controls and guidance for information governance, security, control, and audit professionals. This international association focuses on IT governance, providing benchmarks and governance tools for organizations that employ information systems. ISACA is behind the creation, sponsorship, and driving of the COBIT framework.

ISACA has served our professional community for more than 50 years. The association was incorporated as the EDP Auditors Association in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the new field of electronic data processing audit. Today, ISACA serves 145,000 professionals in 180 countries, who span several roles in assurance, governance, risk and information security.” <https://www.isaca.org/why-isaca/about-us>

Internal Auditing – IIA’s definition “Internal auditing is an independent, objective, assurance and consulting activity designed to add value and improve an organization’s operations. At its

simplest, internal audit involves identifying the risks that could keep an organization from achieving its goals, making sure the organization's leaders know about these risks, and proactively recommending improvements to help reduce the risks." Additionally, "Internal auditors are explorers, analysts, problem-solvers, reporters, and trusted advisors. They bring objectivity and a variety of skills and expertise to the organization." <https://global.theiia.org/about/about-internal-auditing/pages/about-internal-auditing.aspx>

Internal Control – "A plan of organization under which employees' duties are arranged, and records and procedures are designed, to make it possible to exercise effective control over processes. Internal control procedures which call for proper authorizations by designated officials for all actions performed that must be specified and followed." <https://global.theiia.org>

International Organization for Standardization (ISO) – "Organizations subordinate to federal agencies may use the term Senior Information Security Officer or Chief Information Security Officer to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.

<https://csrc.nist.gov/glossary/term/iso> National Institute of Standards and Technology

National Center for Education Statistics (NCES) – "Is the primary federal entity for collecting and analyzing data related to education in the U.S. and other nations. NCES is located within the U.S. Department of Education and the Institute of Education Sciences. NCES fulfills a Congressional mandate to collect, collate, analyze, and report complete statistics on the condition of American education; conduct and publish reports; and review and report on education activities internationally." <https://nces.ed.gov/about/>

National Institute of Standards and Technology (NIST) – "The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals." www.nist.gov

Information Technology Laboratory (ITL) – "The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf>

Organizational Chart – "Organizational charts are the presentation of reporting relationships and employee roles in an enterprise. A well-structured organizational structure would help improve

productivity, but a poor organizational structure can weak the organization.”

<https://www.orgcharting.com/poor-organizational-structure/>

Plagiarize: To steal and pass off (the ideas or words of another) as one’s own: use (another’s productions) without crediting the source. Marriam Webster, since 1828, <https://www.merriam-webster.com/dictionary/plagiarizing>

Prevention - “Prevention - To prevent, avoid, or stop a crisis event from happening in a school environment.” 2022 -Arizona Department of Education - <https://www.azed.gov/wellness/sep>

Protection – “To protect all individuals in a school environment against the greatest threats and hazards to them in their specific school's environment.” 2022 -Arizona Department of Education - <https://www.azed.gov/wellness/sep>

Ready – “Launched in February 2003, Ready is a National public service campaign designed to educate and empower the American people to prepare for, respond to and mitigate emergencies, including natural and man-made disasters.” <https://www.ready.gov>

Response – “To respond to any crisis event on a school campus quickly to save lives, protect the school's property and environment, and meet basic human needs in the aftermath of a catastrophic event. 2022 -Arizona Department of Education.” - <https://www.azed.gov/wellness/sep>

Recovery – “To recover through a focus on the timely restoration, strengthening and revitalization of infrastructure, housing and a sustainable economy, as well as the health, social, cultural, historic and environmental fabric of communities affected by a catastrophic incident.” 2022 -Arizona Department of Education - <https://www.azed.gov/wellness/sep>

The Institute of Internal Auditors (IIA) – “Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession’s global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.”

<https://na.theiia.org/standards-guidance/Member%20Documents/PG-Business-Continuity-Management.pdf>

U.S. Department of Education (DOE) – “Is the agency of the federal government that establishes policy for, administers and coordinates most federal assistance to education. It assists the president in executing his education policies for the nation and in implementing laws enacted by Congress.” <https://www2.ed.gov>

United States Government Accountability Office (GAO) – “GAO, often called the “congressional watchdog,” is an independent, non-partisan agency that works for Congress. GAO examines how taxpayer dollars are spent and provides Congress and federal agencies with objective, non-partisan, fact-based information to help the government save money and work more efficiently.” <https://www.gao.gov/about>



TUCSON UNIFIED SCHOOL DISTRICT

Technology Services Responses to DRPBCP Internal Audit Report

DATE: August 2022

PREPARED BY:

Rabih Hamadeh – Interim Executive Director of Technology Services, TUSD

REVIEWED BY:

Blaine Young – Chief Operations Officer, TUSD

Rabih Hamadeh – Interim Executive Director of Technology Services, TUSD

SUMMARY

The Technology Services (TS) Department recognizes and appreciates the work done by Ms. Martha Smith, the Internal Auditor for Tucson Unified School District, to complete this audit report. We have discussed the report's findings and observations with our teams and are providing in this document relevant responses and feedback.

The TS Department has prepared and provided for this audit a full and comprehensive Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) in July 2022. Fourteen documents were provided in total. Some of the documents are provided as appendices supporting the TS responses.

The Technology Services Department Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) of July 2022, like many technology DRPs and BCPs is intended to be implemented, when there is a need, by Information Technology (IT) Subject Matter Experts (SMEs) only, and not by the general audience. This concept of only IT SMEs performing complex IT troubleshooting has to be strictly required and enforced.

We at the TS department are committed to providing exceptional technology support for our District, and are constantly searching for ways and best practices to improve and update our systems, processes and support models, including Disaster Recovery Plans (DRP) and a Business



TUCSON UNIFIED SCHOOL DISTRICT

Continuity Plans (BCP). While recognizing there are areas that need review and improvement, the main remark by the TS team regarding most of the findings of this audit is that the audit finds it necessary to deem incomplete or inaccurate some of the information in the TS DRP and BCP, rather than recognizing that there is not a unique way to present the information. The additional perception by the audit findings is that there needs to be more explanations for some of the DR and BC methods and processes. This is based on an incorrect assumption that the DRP and BCP should be implemented by non-IT personnel, when in reality, only IT personnel should, and must, execute the required steps needed for disaster recovery and business continuity. This concept and practice of IT professionals attending to IT tasks is universally supported by all IT organizations and related industries. The TS team is willing to continue the discussion with the internal auditor and all stakeholders, to ensure that the best IT service is provided to our District and its students and staff.

It is important to recognize that the District successfully operated all business functions and instructional delivery in a business continuity mode of operation from March 2020 to the present time (August 2022) during the COVID-19 pandemic. Instructional delivery has continued to occur remotely and on premise for a large portion of the student population. These accomplishments clearly demonstrate that the Technology Services team, district departments and school campuses can, and have achieved, successful business continuity execution. The TS department teams have also successfully performed many disaster recovery and business continuity resolutions over the years. As a result, the content of the DRP and BCP document was based on actual achievements and experiences over the years, and not limited to theoretical approaches and assumptions. During the Internal Audit Exit Meeting, Ms. Smith offered to provide an “excellent plan” from a similar size school district as an example of what she believes should be in place. TS requested that Ms. Smith please provide that document and our team would be happy to review and incorporate updates where it would benefit TUSD’s DRP/BCP.



TUCSON UNIFIED SCHOOL DISTRICT

TECHNOLOGY SERVICES' RESPONSES: (INTERNAL AUDIT REPORT #001_FY2022-2023)

1. Audit Report Observation #1: "No Departmental Policies and Procedures".

Technology Services Department Response:

- The Technology Services (TS) Department Disaster Recovery Plan (DRP) & Business Continuity Plan (BCP), July 2022 (TS DRP & BCP, July 2022) is a full and comprehensive document. For a full review, please refer to the document that was provided for this audit (Appendix A: *Audit-TS-DRBC-1-DRPBCP-July2022*).
- The TS DRP & BCP, July 2022 does self-document when and how the plan is used and when plan updates are made.
- The TS DRP & BCP, July 2022 includes all relevant DR and BC procedures and processes.
- The TS DRP & BCP, July 2022 follows acceptable standards and better business practices of the Information Technology (IT) industry, including but not limited to the Information Technology Infrastructure Library (ITIL), The International Standards Organization (ISO) and the Institute of Electrical and Electronic Engineers (IEEE).
- The TS DRP & BCP, July 2022 follows one of the many formats used for DRPs and BCPs. The format and contents of a DRP and BCP are not unique, and vary based on many industry factors.
- The TS DRP & BCP, July 2022 and its supporting documents include in details all the required and relevant DR and BC information, including but not limited to: Dedicated Team Info; Disaster Risks, Critical Hardware, Software, Applications, Resources; On-Site and Off-Site Data Center and Backup Locations.
- Audit Recommendations a and b have been addressed in the TS DRP & BCP, July 2022, and in this response. The recommendations will be reviewed further and improvements will be made if needed in the updated DRP and BCP.



TUCSON UNIFIED SCHOOL DISTRICT

2. **Audit Report Observation #2:** “Limited Information and Content in TS’s DRP/BCP”.

Technology Services Department Response:

- The Technology Services (TS) Department Disaster Recovery Plan (DRP) & Business Continuity Plan (BCP), July 2022 includes, but is not limited to, the following information:
 - Overview/Scope
 - Technology Services Team and District Team including titles, contact information and responsibilities
 - List of Vendors with all relevant information
 - Records and Vital Documents
 - Essential Systems Information
 - Definition of and implementation processes for basic DR and BC tools such as recovery Point Objectives (RPO), Recovery Time Objectives (RTO) and Tiers
 - Systems Architecture, Resources, Locations and Applications
- DRPs and BCPs can have many accepted IT industry formats and templates. The plan is not a unique document, with unique outlines and contents.
- Audit Recommendations a - g have been addressed in the TS DRP & BCP, July 2022, and in this response. The recommendations will be reviewed further and improvements will be made if needed in the updated TS DRP & BCP. Recommendation c: the reference is techtarget.com. The reference will be included in the updated TS DRP & BCP
- A few full or partial supporting samples of the content included in the TS DRP & BCP, July 2022 are shown below. For full content, please refer to Appendix A: *Audit-TS-DRBC-1-DRPBCP-July2022*



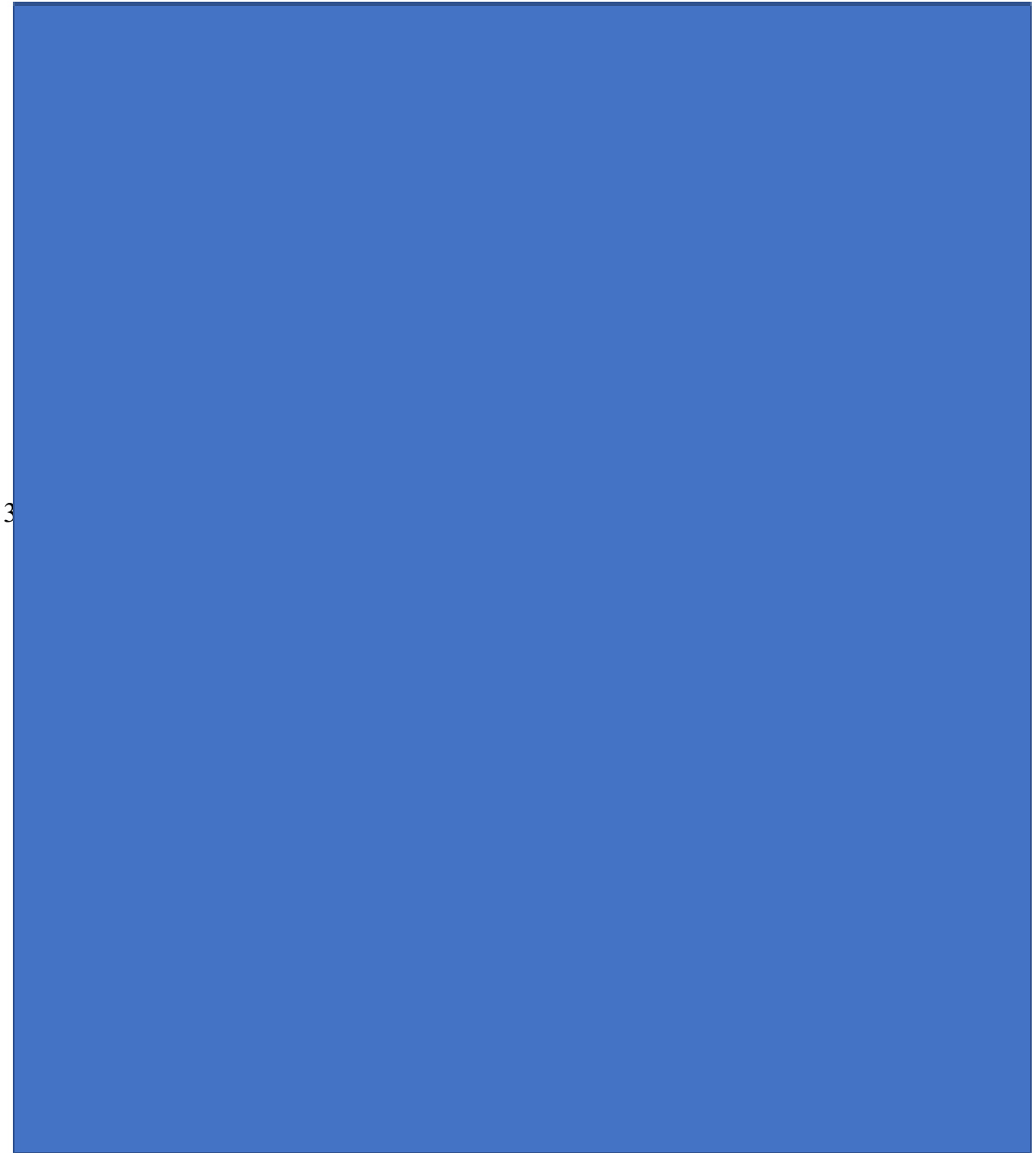
TUCSON UNIFIED SCHOOL DISTRICT

I. Overview





TUCSON UNIFIED
SCHOOL DISTRICT

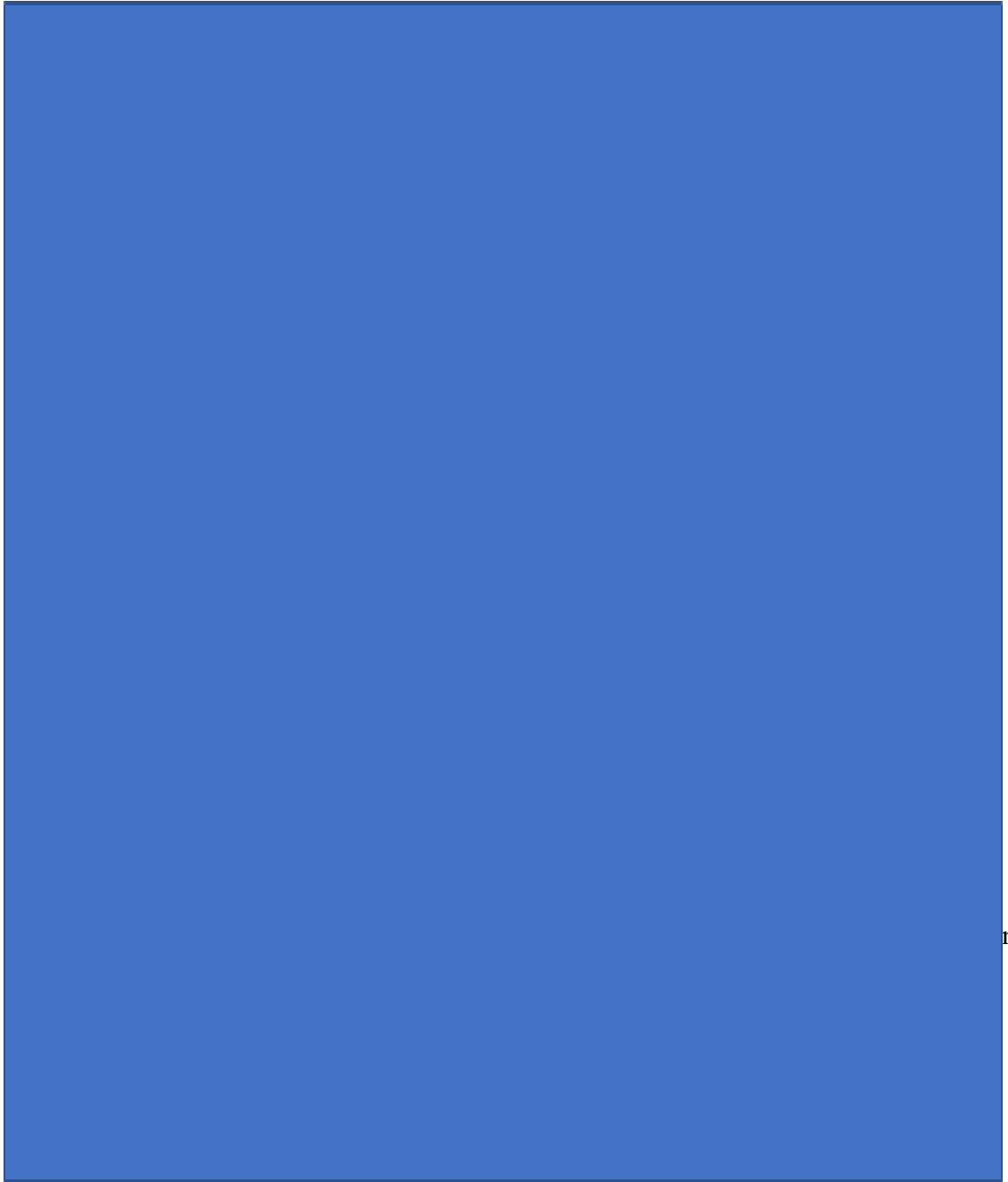


3



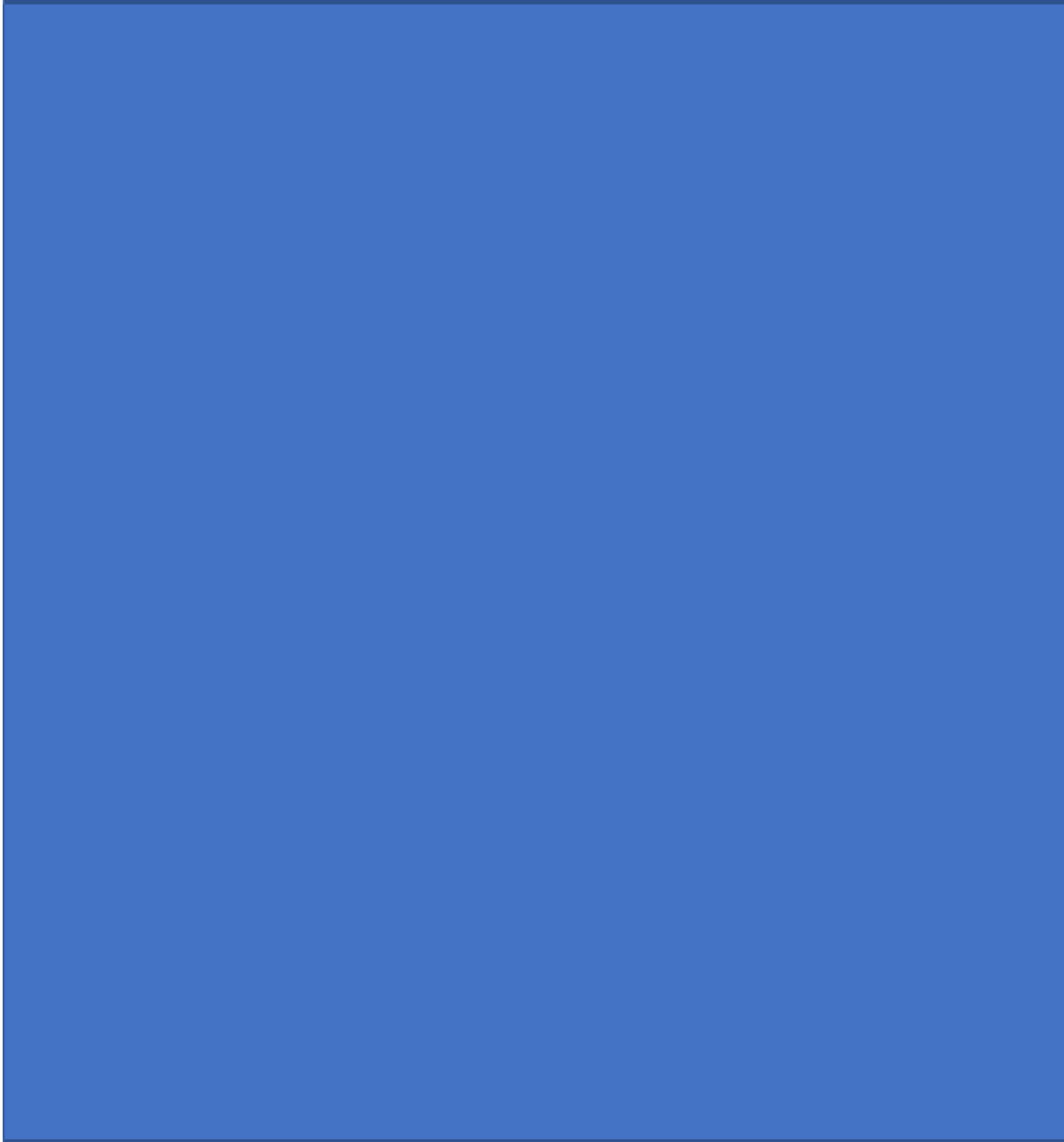
TUCSON UNIFIED

SCHOOL DISTRICT



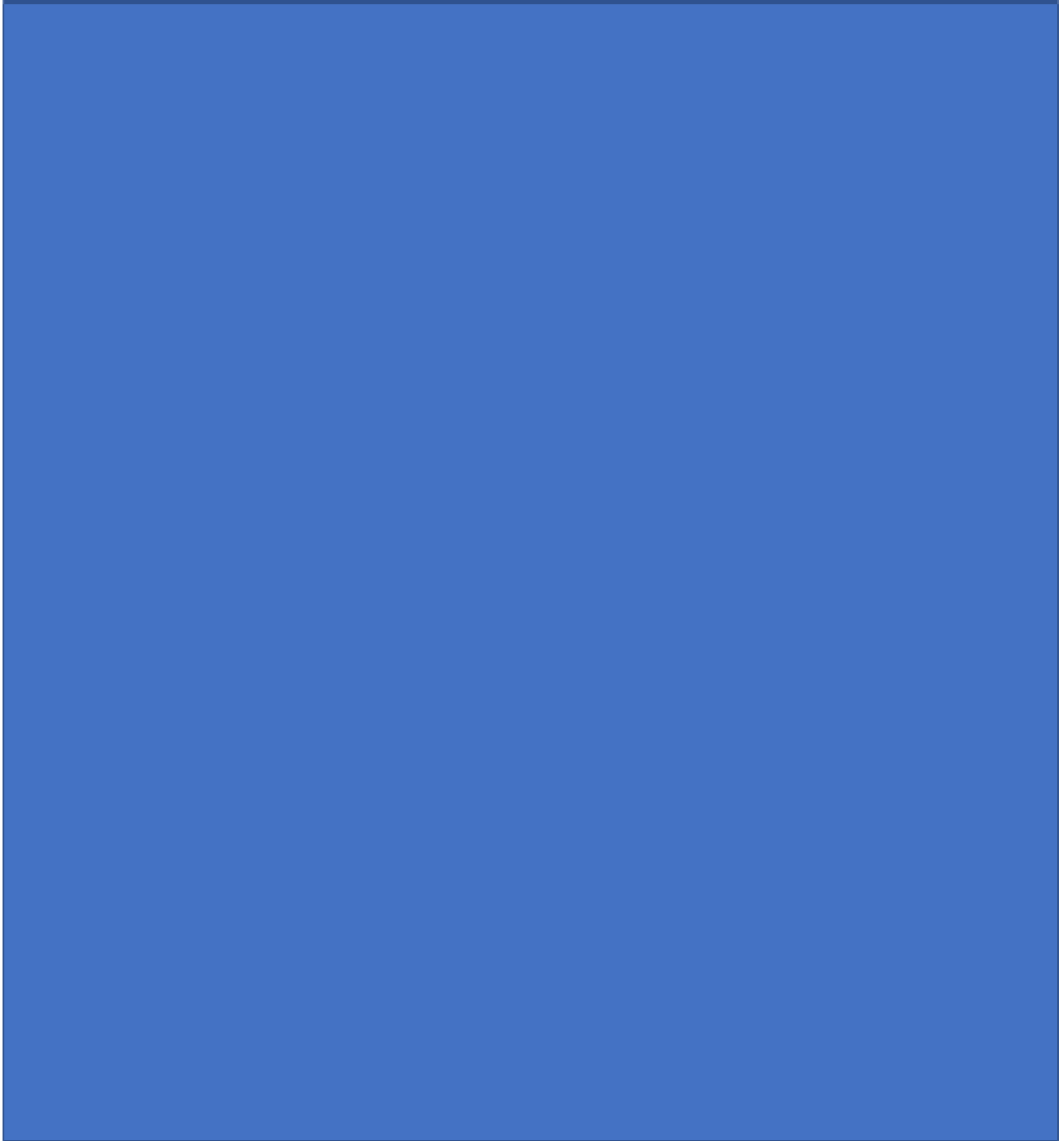


TUCSON UNIFIED
SCHOOL DISTRICT



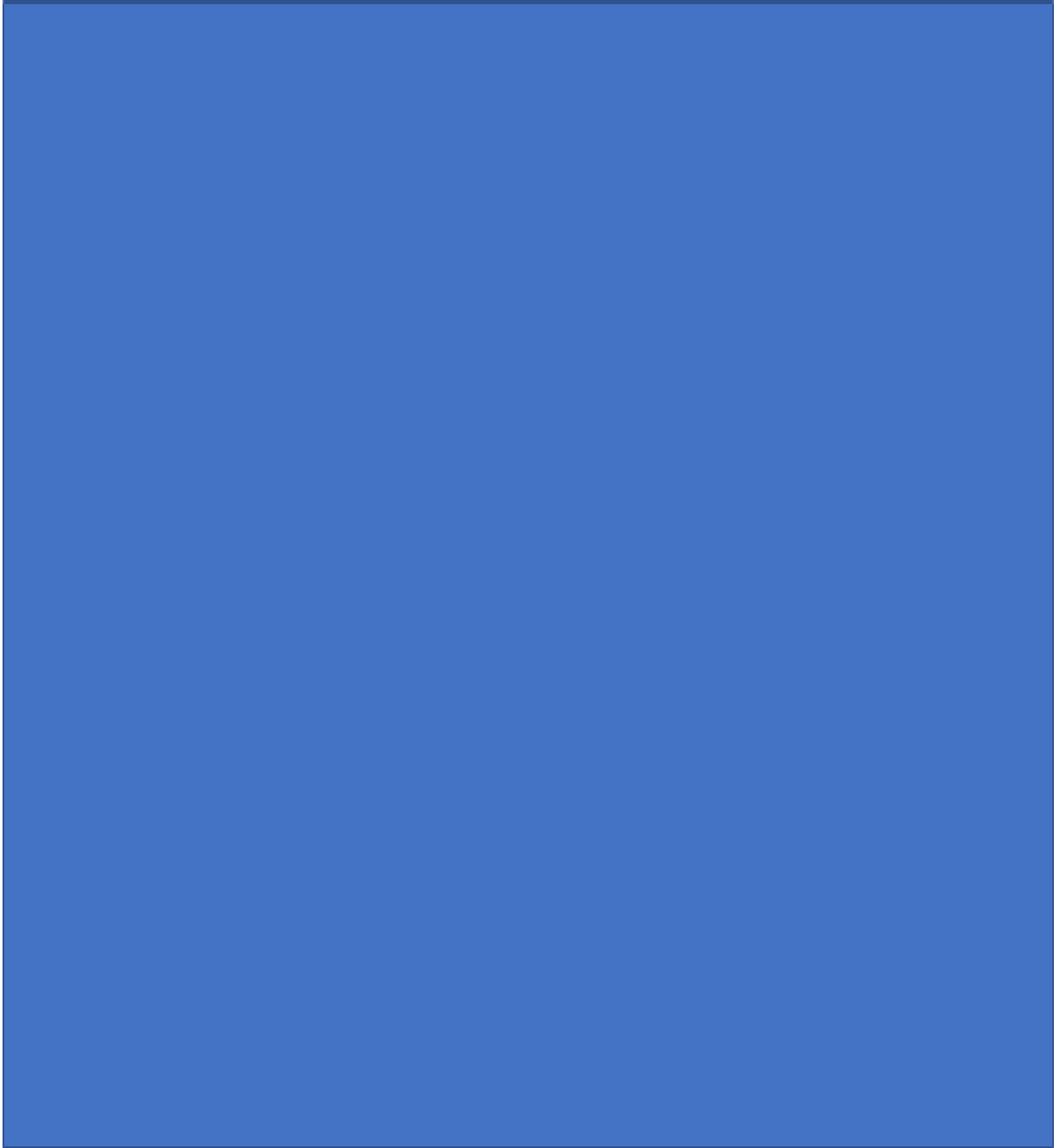


TUCSON UNIFIED
SCHOOL DISTRICT



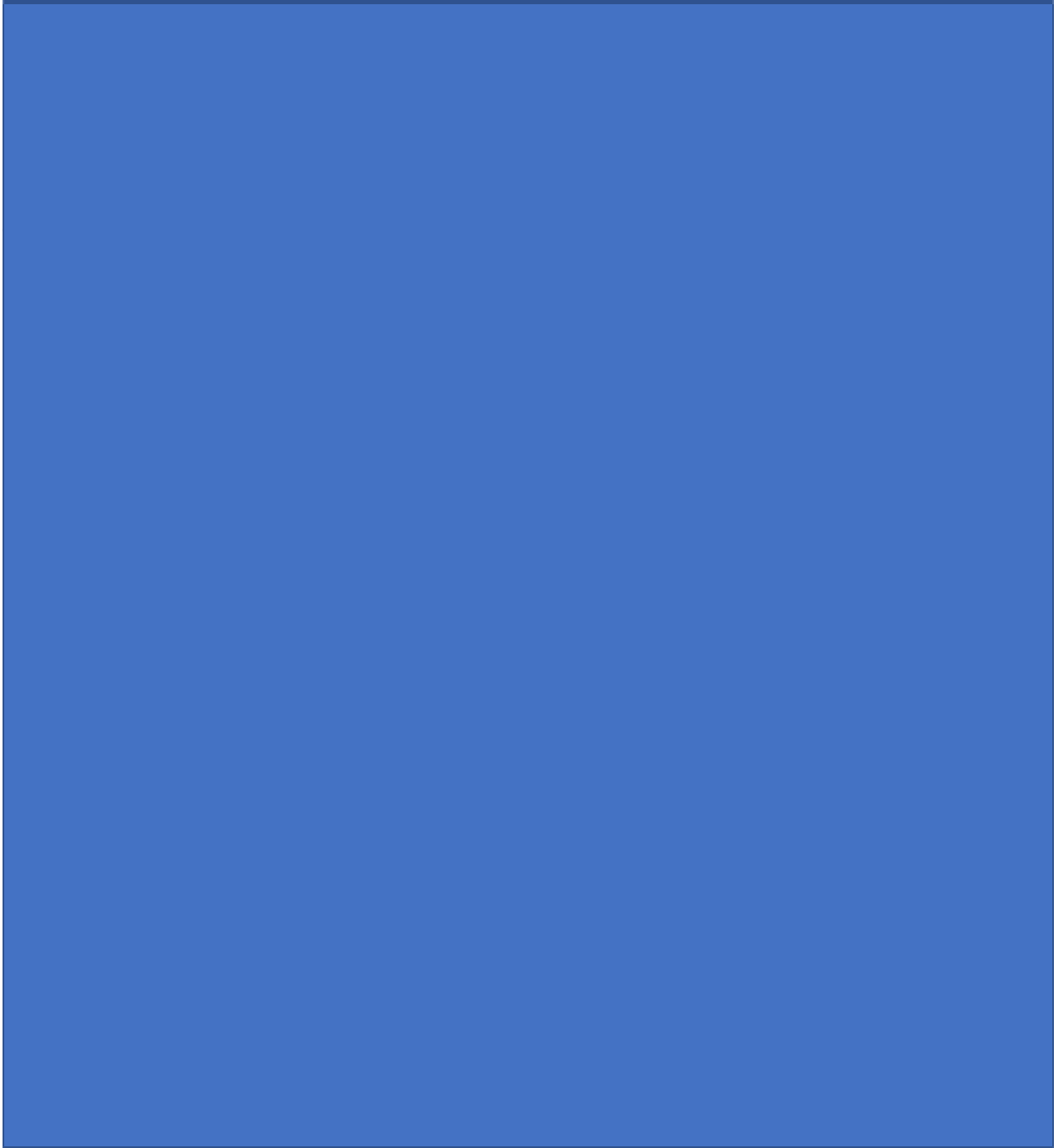


TUCSON UNIFIED
SCHOOL DISTRICT



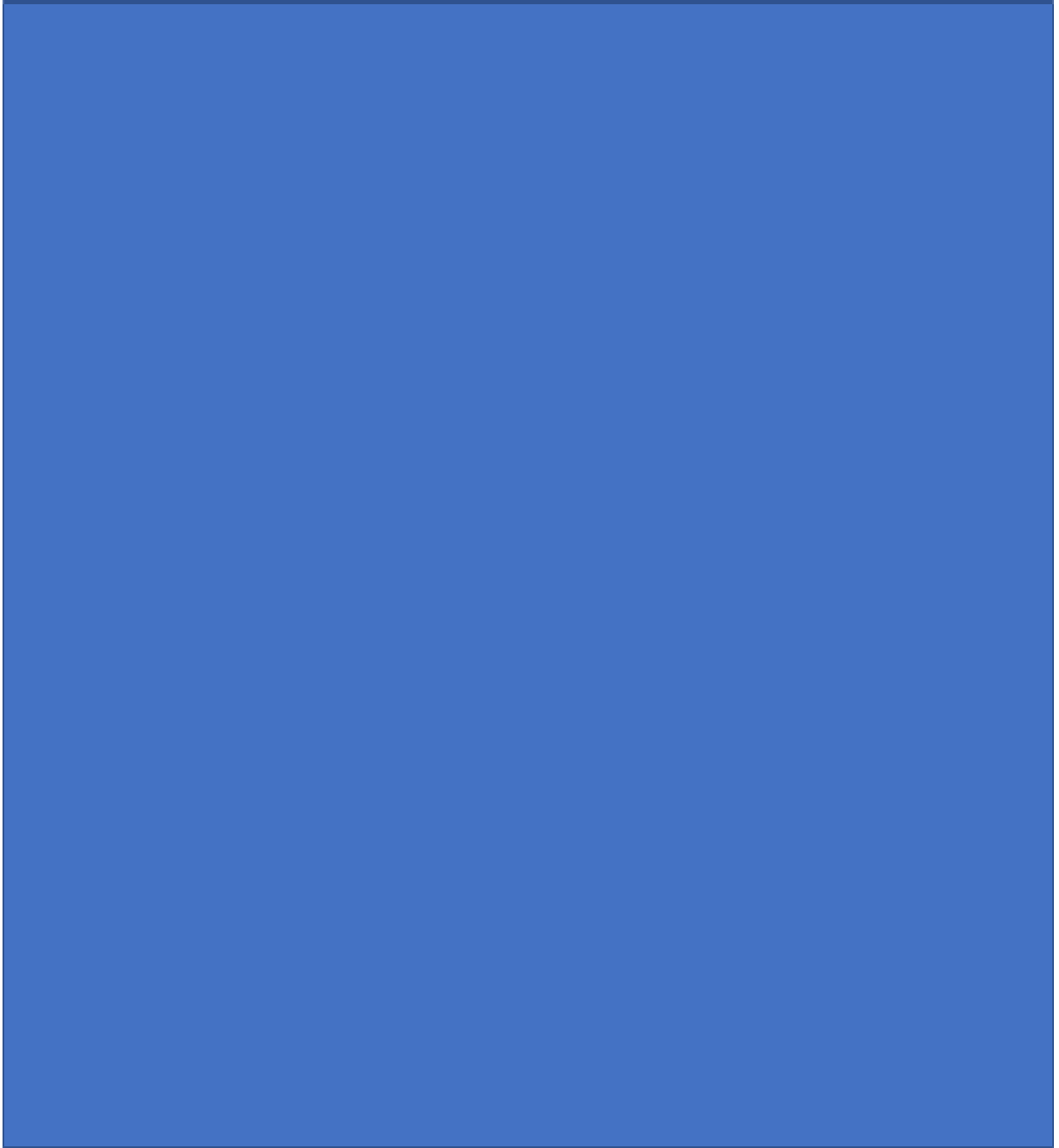


TUCSON UNIFIED
SCHOOL DISTRICT





TUCSON UNIFIED
SCHOOL DISTRICT





TUCSON UNIFIED
SCHOOL DISTRICT

APPENDIX A

Technology Services Department

**Disaster Recovery Plan (DRP)
&
Business Continuity Plan (BCP)**

July 2022





TUCSON UNIFIED SCHOOL DISTRICT

Contents

I.	Overview.....	3
II.	Document Maintenance and Update Requirement.....	3
III.	Disaster Event Declaration.....	3
IV.	Disaster Recovery (DR) & Business Continuity (BC) Team Members and Escalation List.....	4
V.	Accessing Vital Records.....	7
VI.	Systems In-Scope, Recovery Point Objective (RPO),Recovery Time Objective (RTO) & Tiers .	12
A.	Definition.....	8
B.	Tiers.....	8
VII.	Redundancy through Backup and Replication.....	9
VIII.	Network Infrastructure Failover Procedure.....	9
A.	Site Uplink Routers.....	10
B.	Branch Site Virtual Private Network (VPN).....	11
C.	Firewall, Client VPN, Load Balancer.....	11
D.	Internet Router.....	11
IX.	Applications Replication and Failover Strategy.....	11
A.	Domain Controllers Failover.....	11
B.	Applications Failover Conditions and Requirements.....	11
C.	Assumptions and Prerequisites.....	11
X.	Evaluation and Failover Status Check.....	12
A.	Failover Report.....	12
B.	Measuring Recovery Point Objective (RPO), and Recovery Time Objective (RTO).....	12
XI.	Monitoring and Operations Procedure during Disaster.....	13
A.	Team assignment and Logistics at the DR & BC Data Center.....	13



TUCSON UNIFIED
SCHOOL DISTRICT

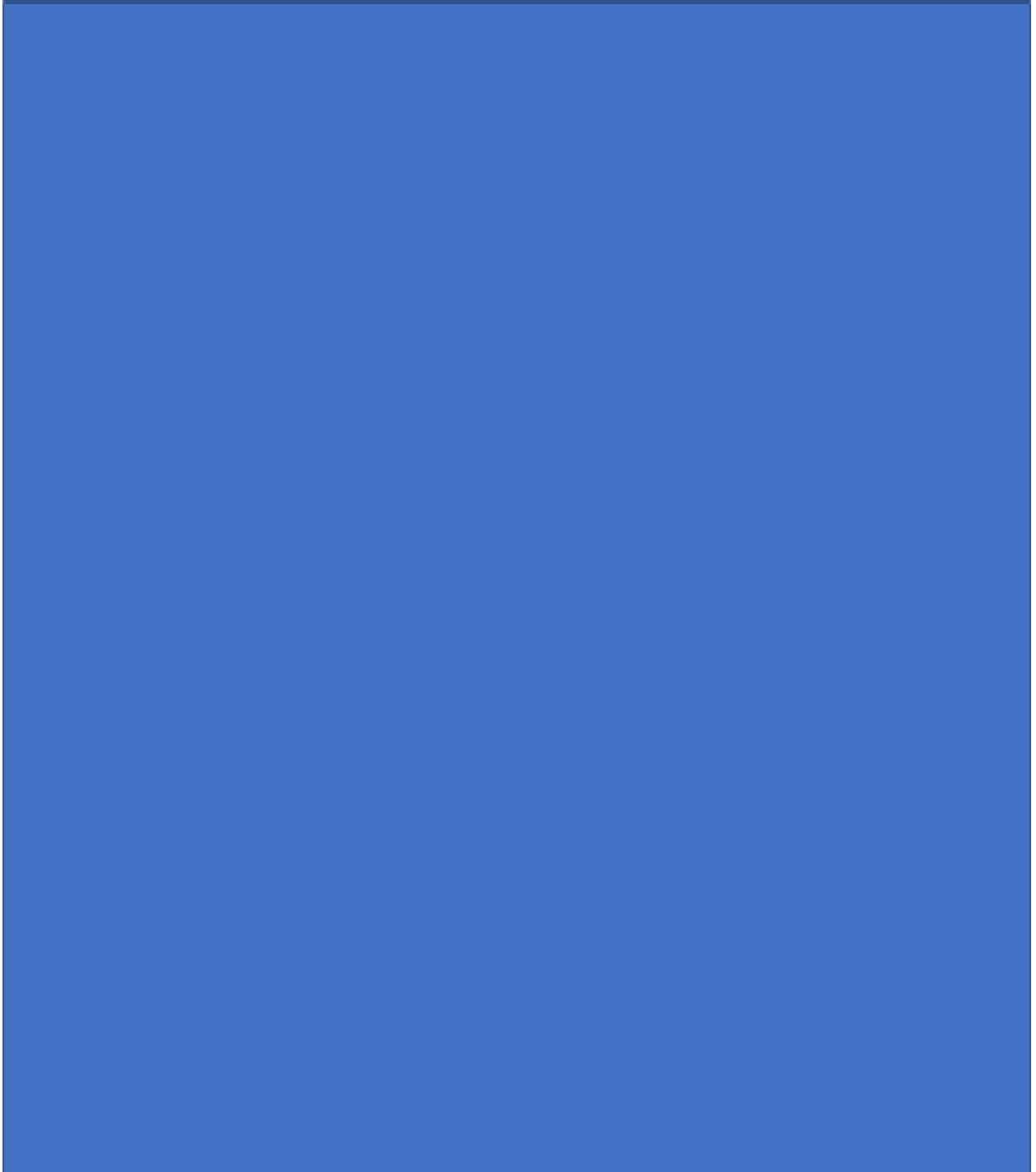
B. User communications and Manual Procedures 13

XII. DR & BC Periodic Testing 13



TUCSON UNIFIED SCHOOL DISTRICT

I. Overview





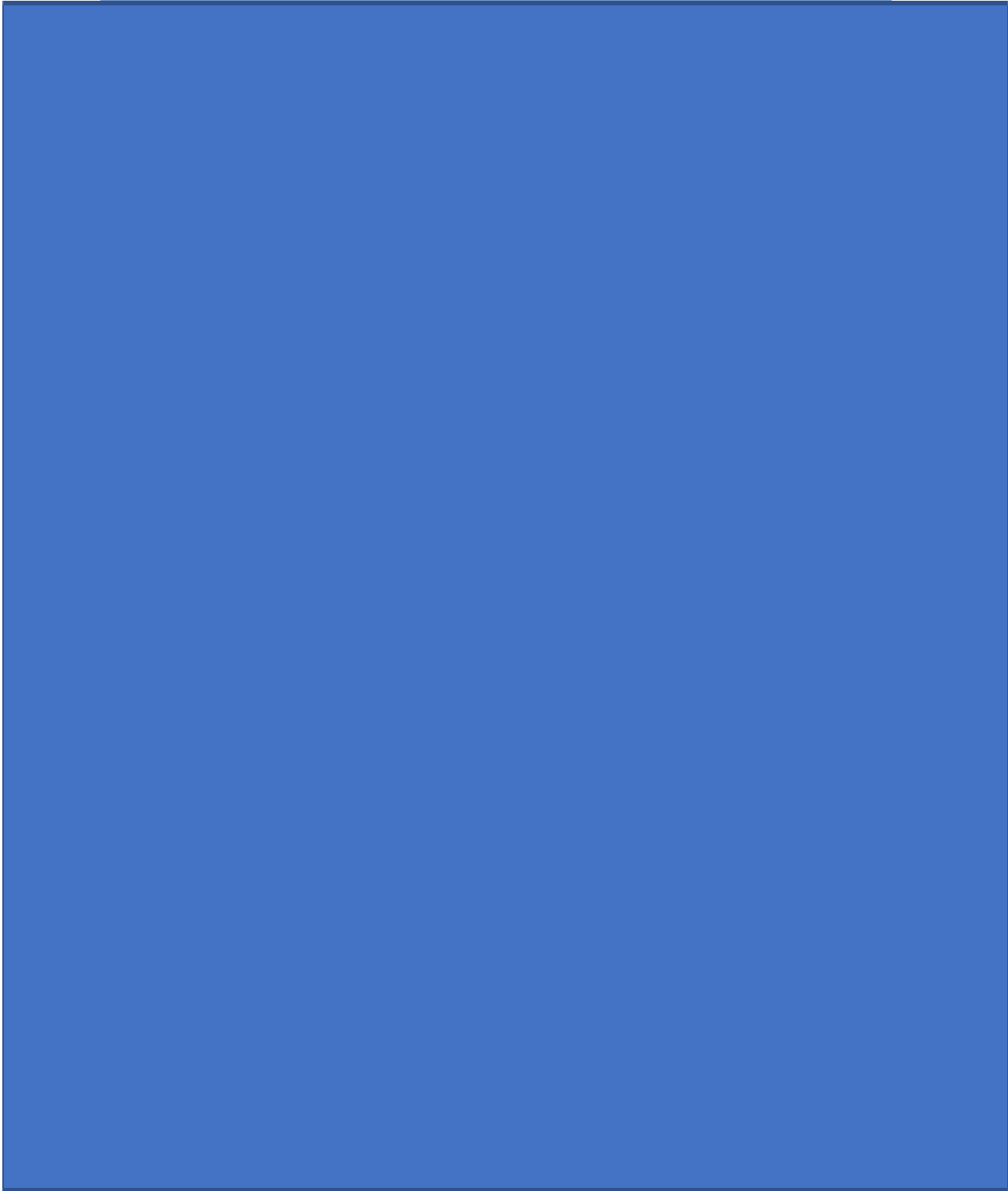
TUCSON UNIFIED
SCHOOL DISTRICT





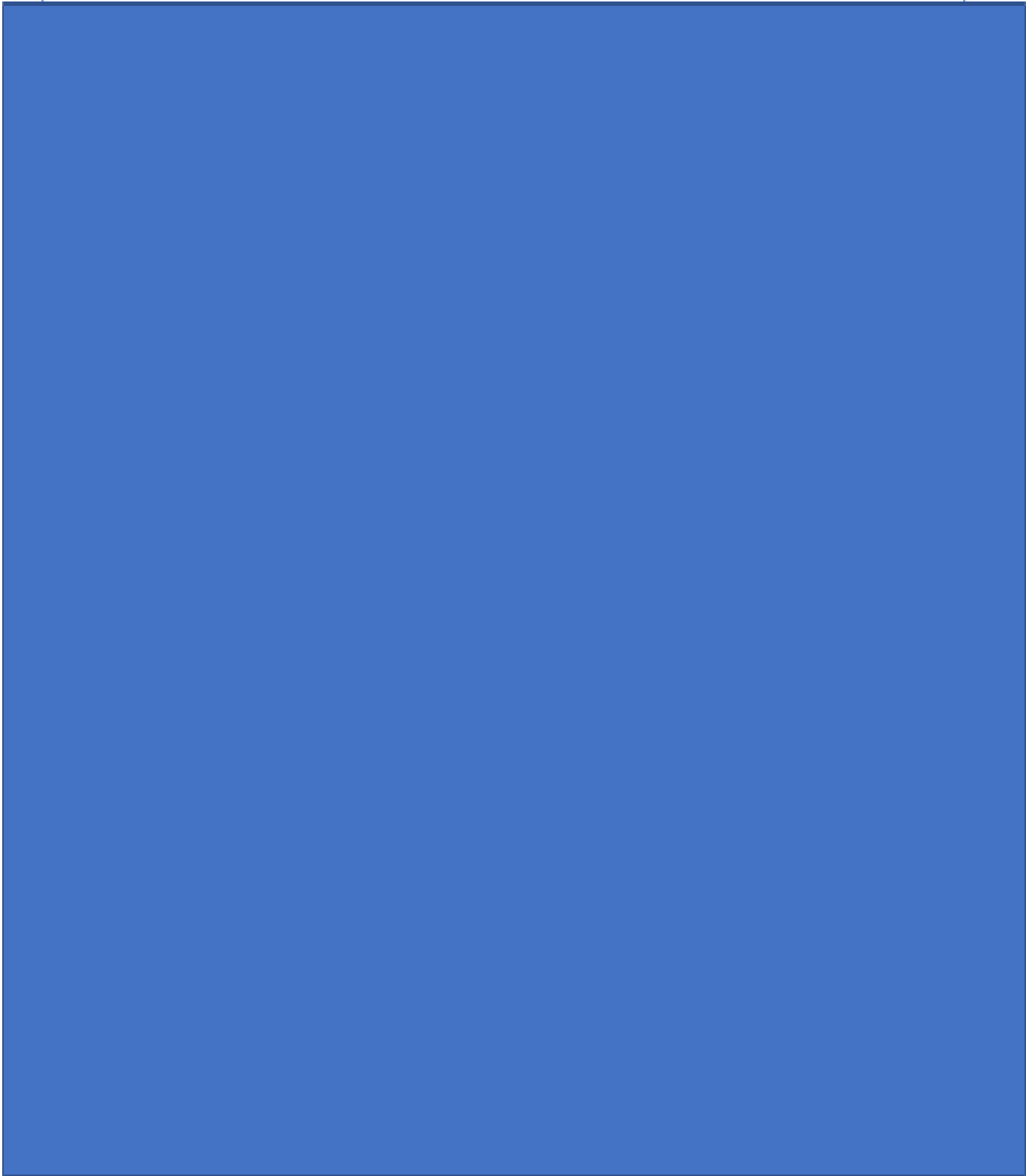
TUCSON UNIFIED

SCHOOL DISTRICT



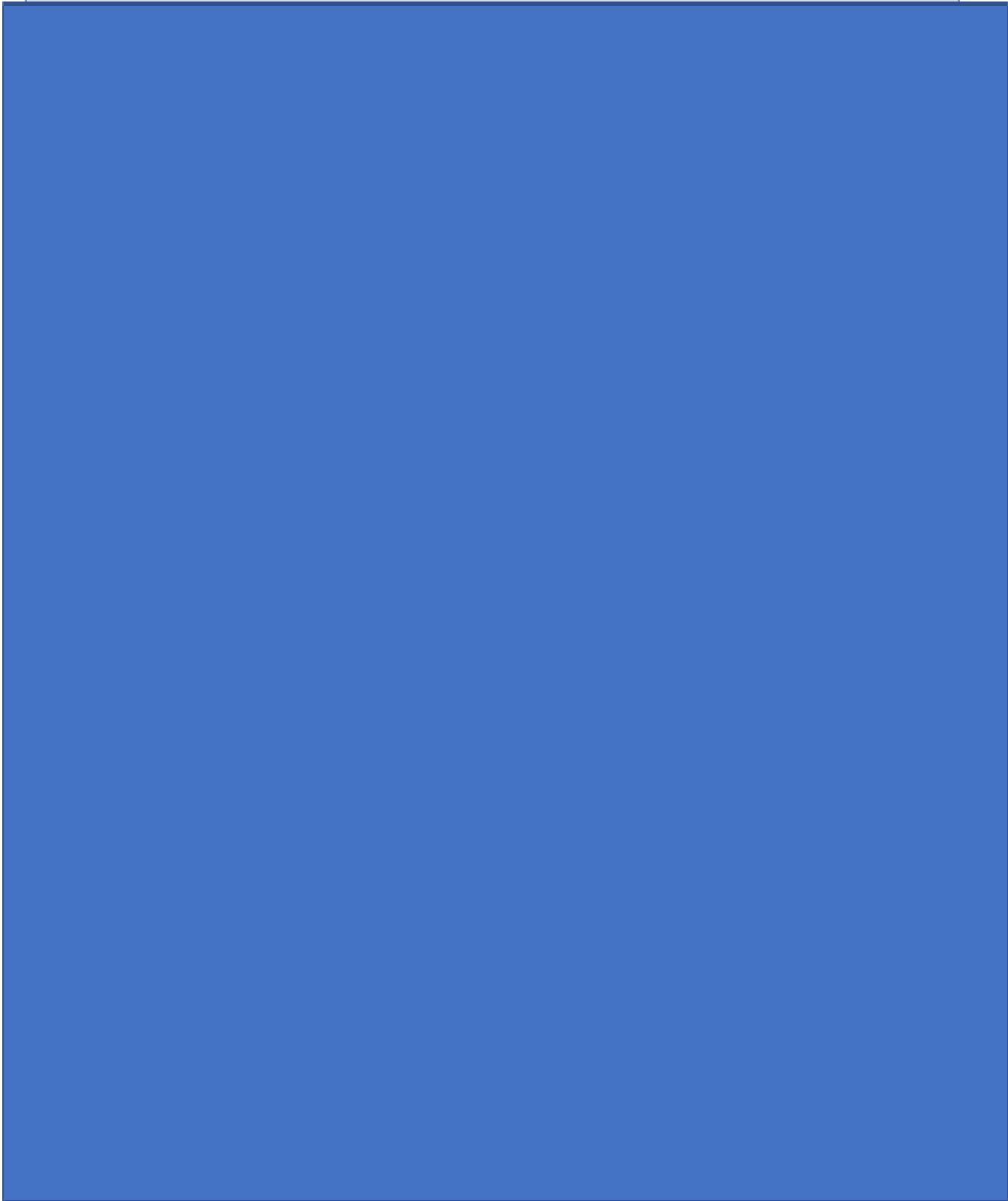


TUCSON UNIFIED
SCHOOL DISTRICT



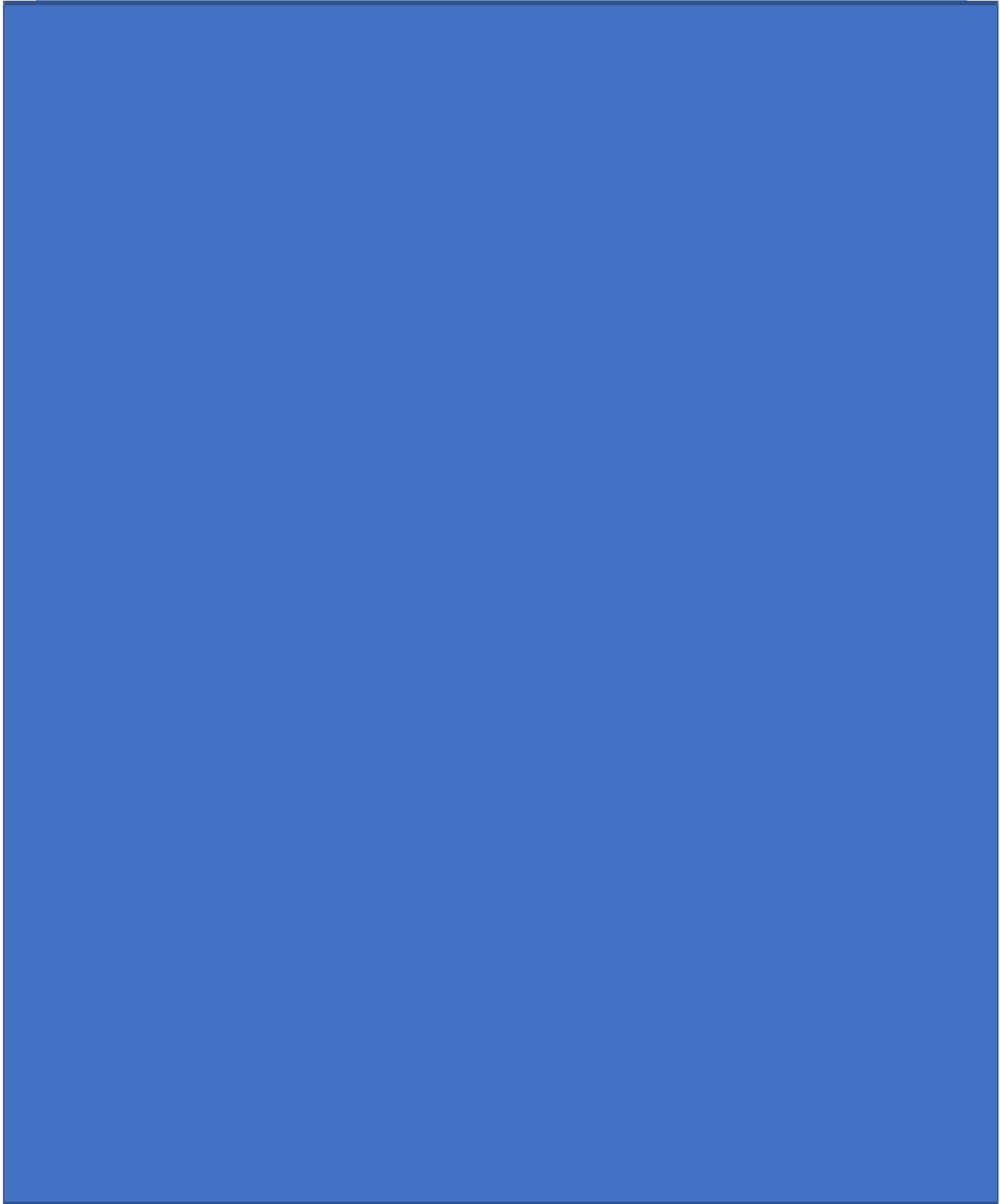


TUCSON UNIFIED
SCHOOL DISTRICT



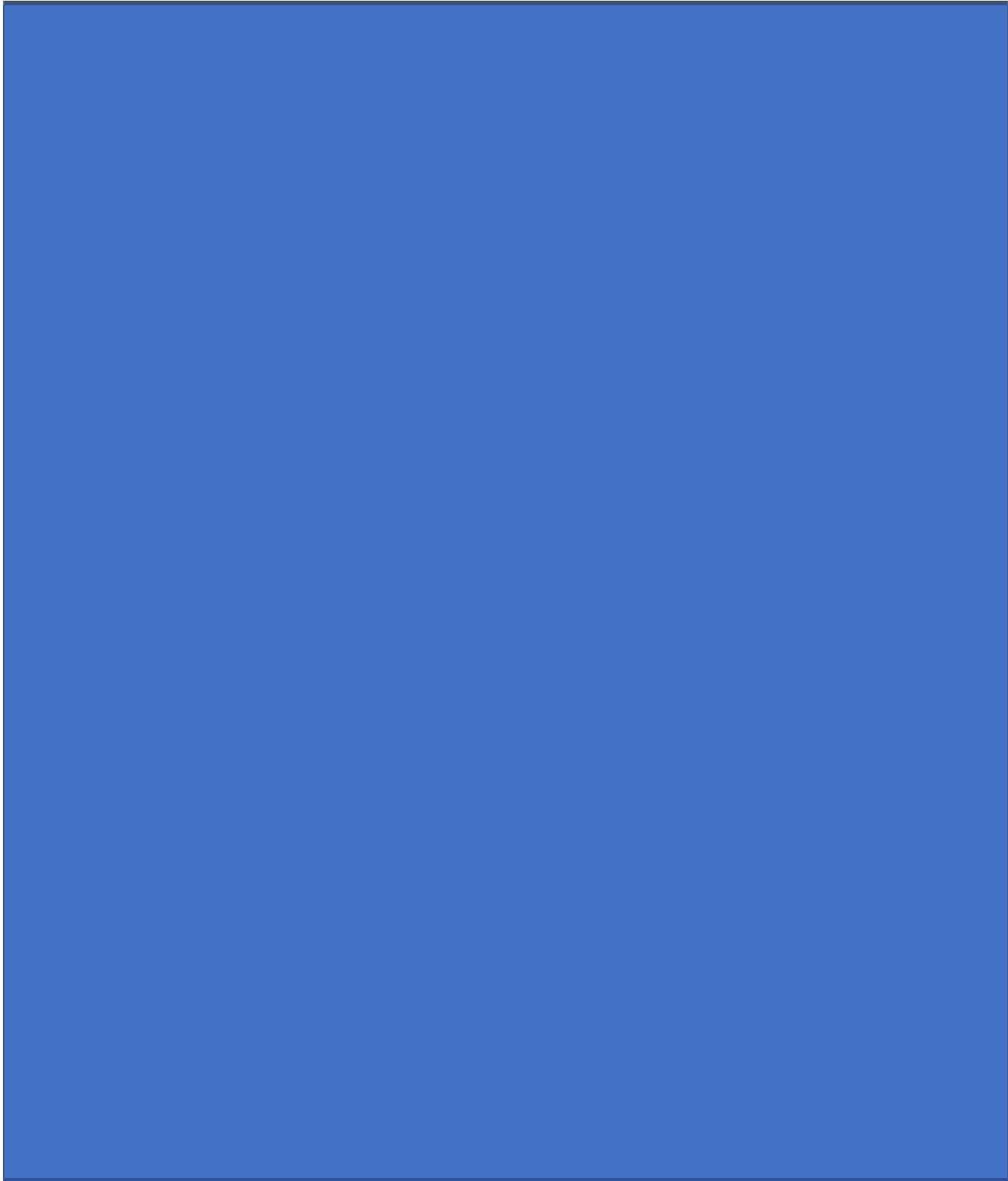


TUCSON UNIFIED
SCHOOL DISTRICT



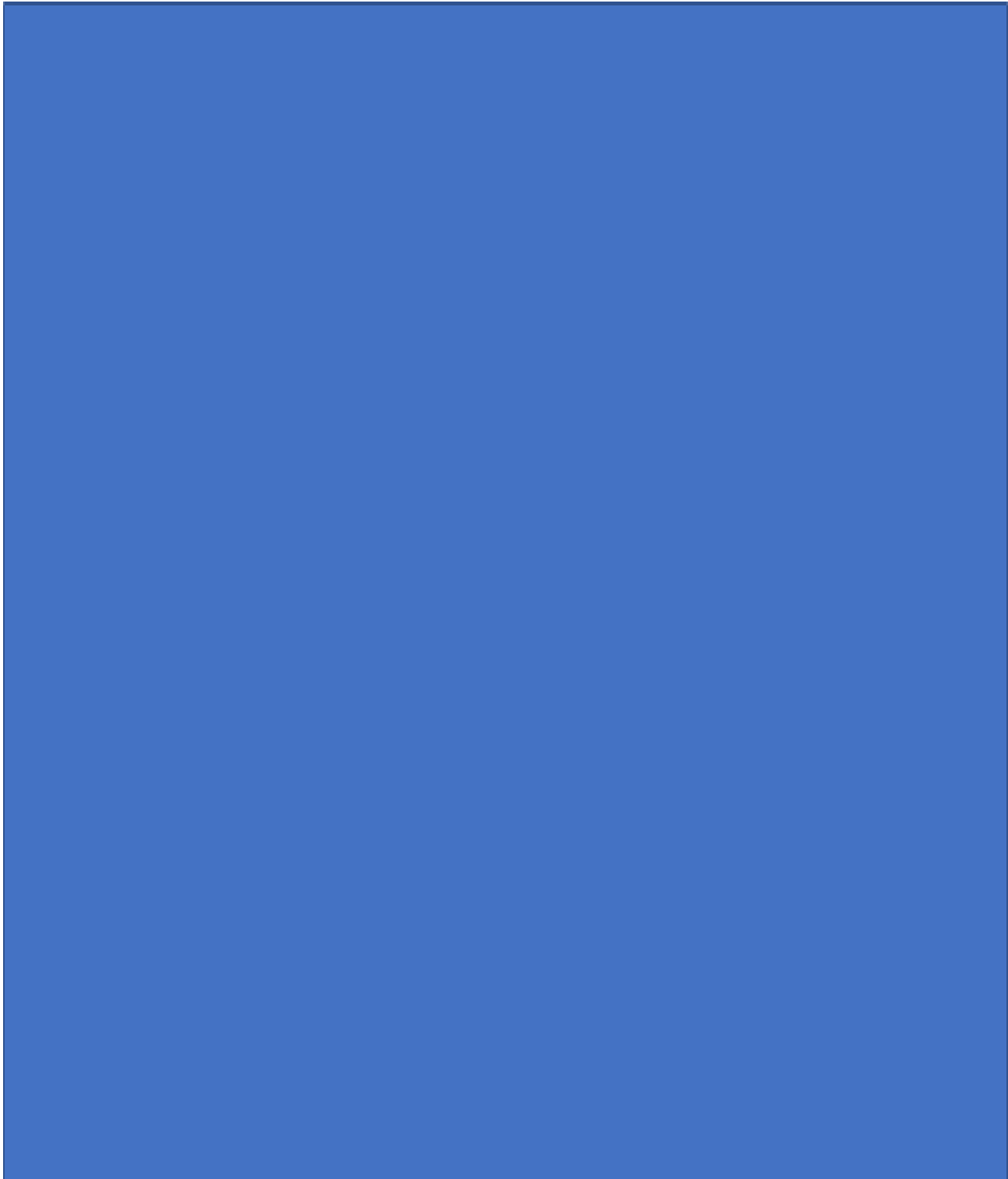


TUCSON UNIFIED
SCHOOL DISTRICT



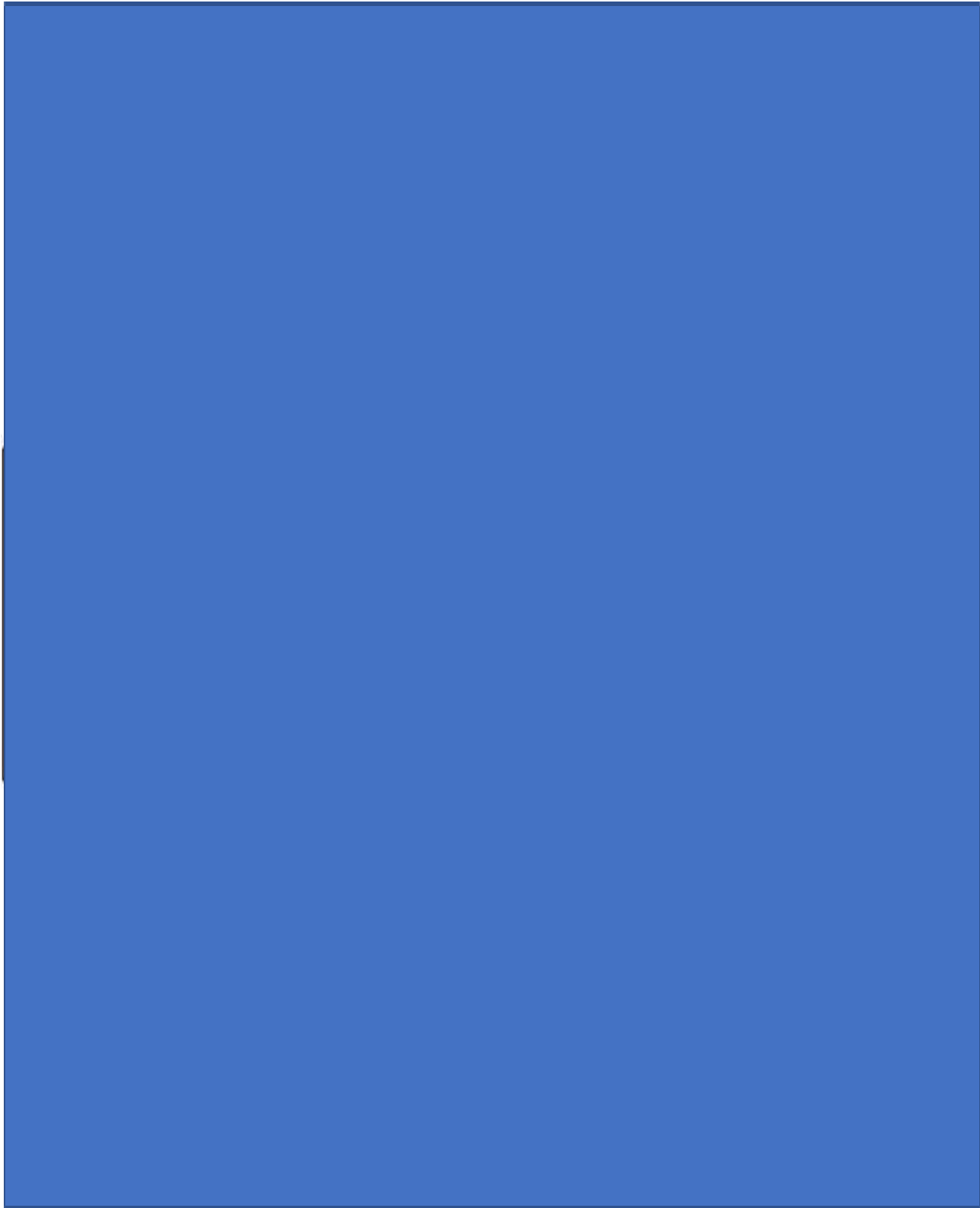


TUCSON UNIFIED
SCHOOL DISTRICT





TUCSON UNIFIED
SCHOOL DISTRICT





TUCSON UNIFIED
SCHOOL DISTRICT





TUCSON UNIFIED

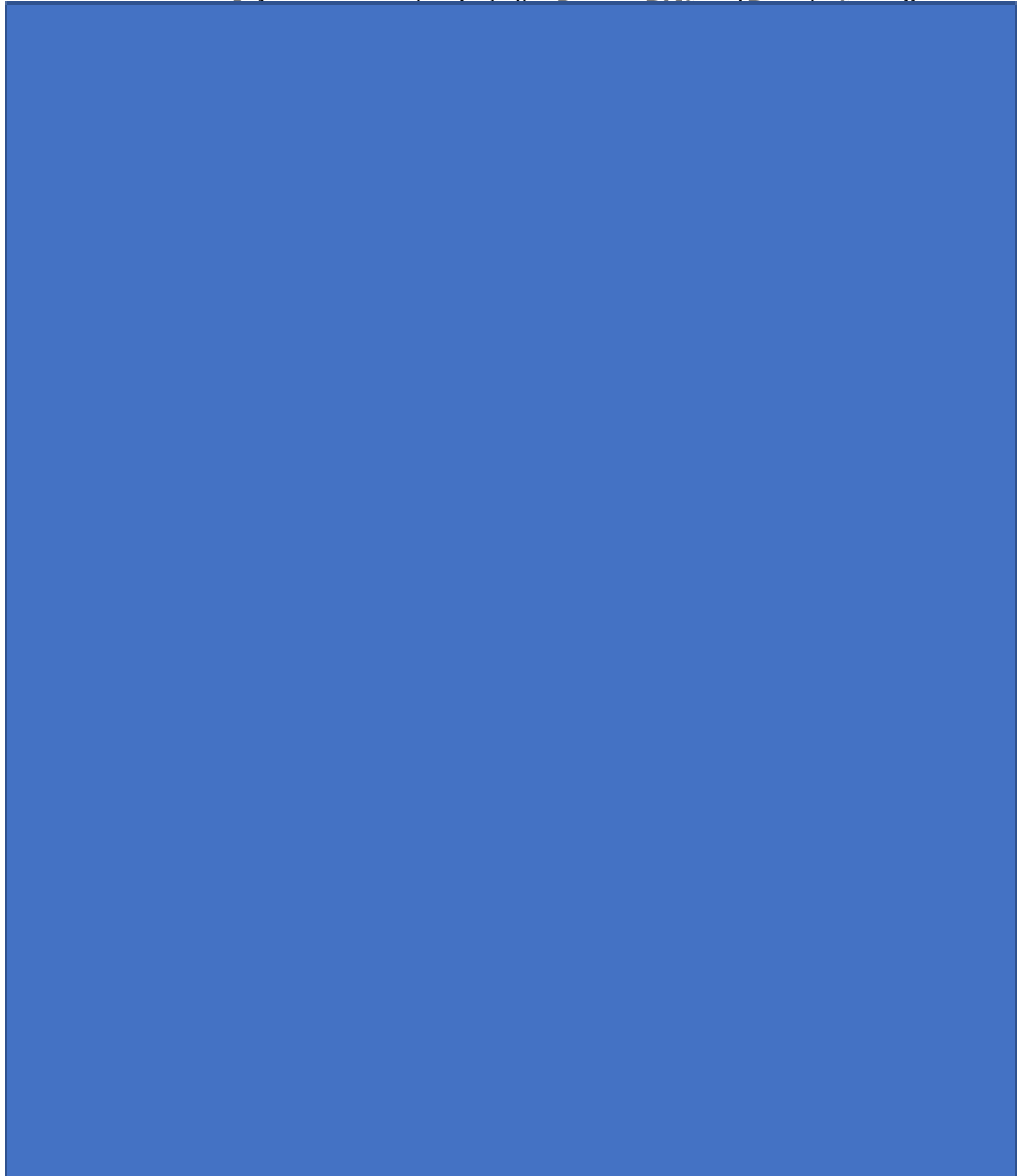
SCHOOL DISTRICT





TUCSON UNIFIED

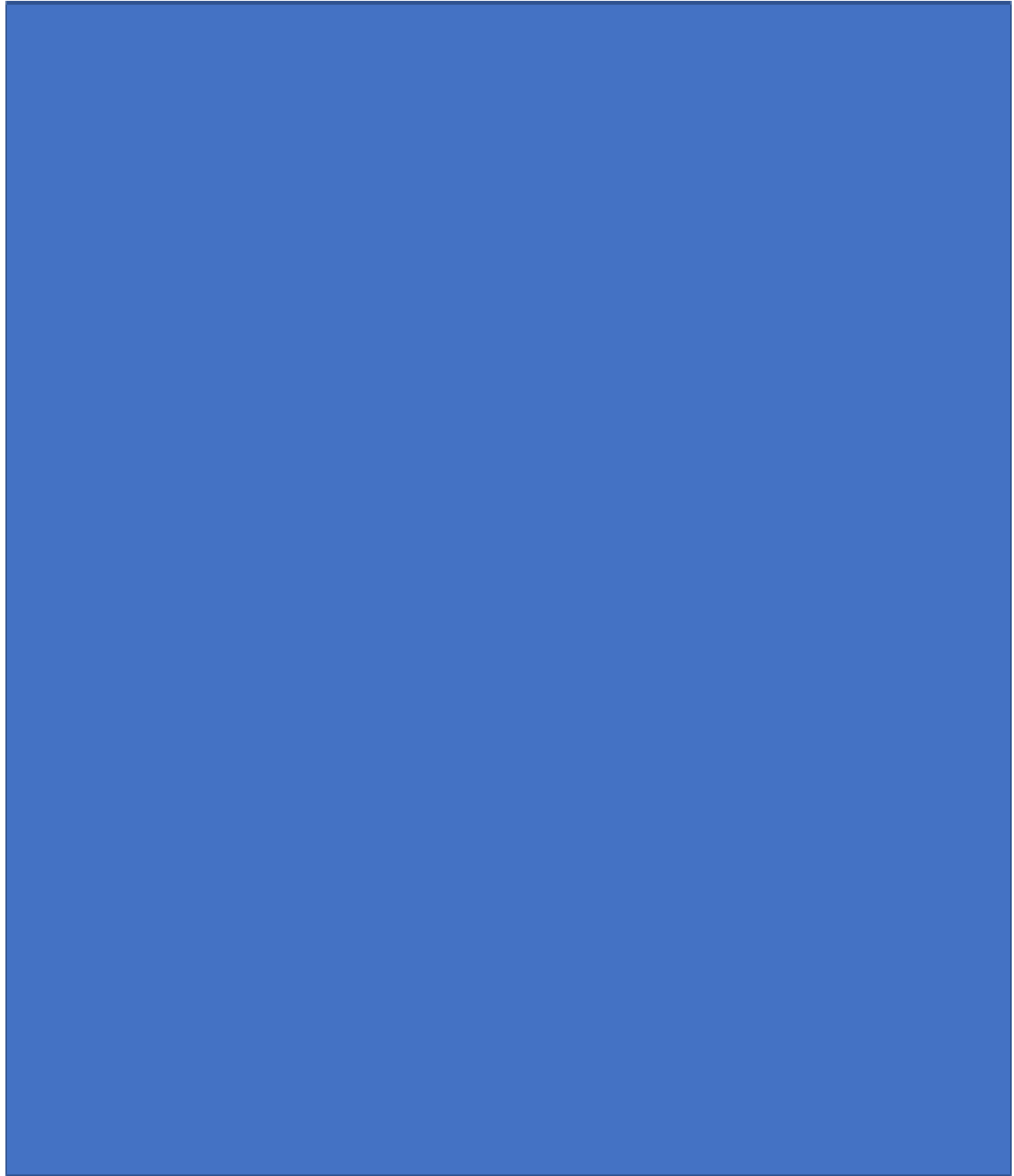
SCHOOL DISTRICT





TUCSON UNIFIED

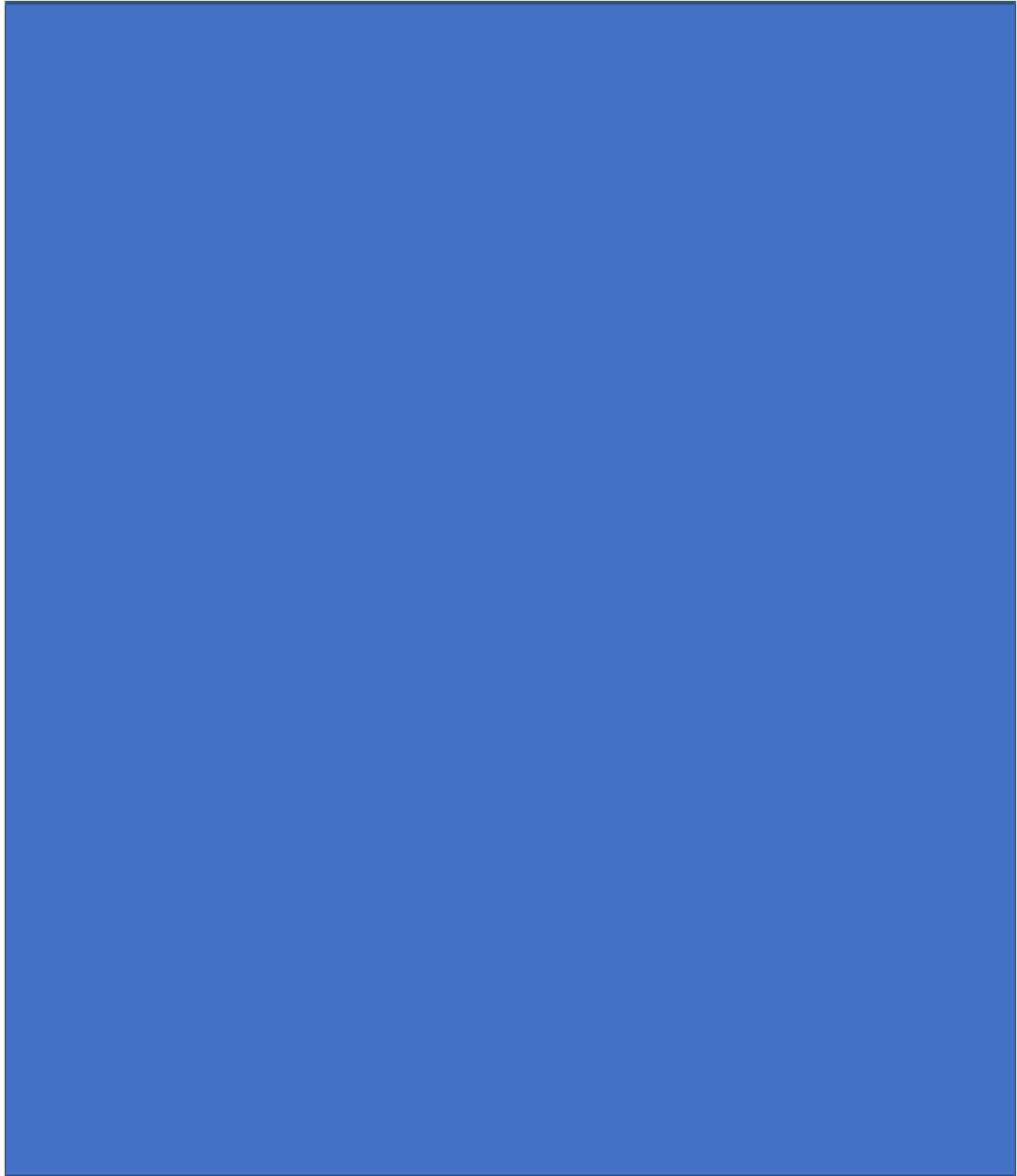
SCHOOL DISTRICT





TUCSON UNIFIED

SCHOOL DISTRICT





TUCSON UNIFIED
SCHOOL DISTRICT

APPENDIX B

Audit Information Sheet

Date: July 2022

Audit Scope: July 1, 2021 to June 30, 2022

Initial Documents Requested:

1. Copy of TS manual for Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) or processes if there are no manuals for DRP/BCP.
2. Copies of TS's policies addressing the DRP/BCP
3. Copies of TS's Operating Standard Procedures for DRP/BCP
4. Copy of the most recently performed test report.
5. Copy of the most recent data backup log for the top five items for both cloud and physical.
6. Most recent Business Impact Analysis (BIA) Report.

Audit Information:





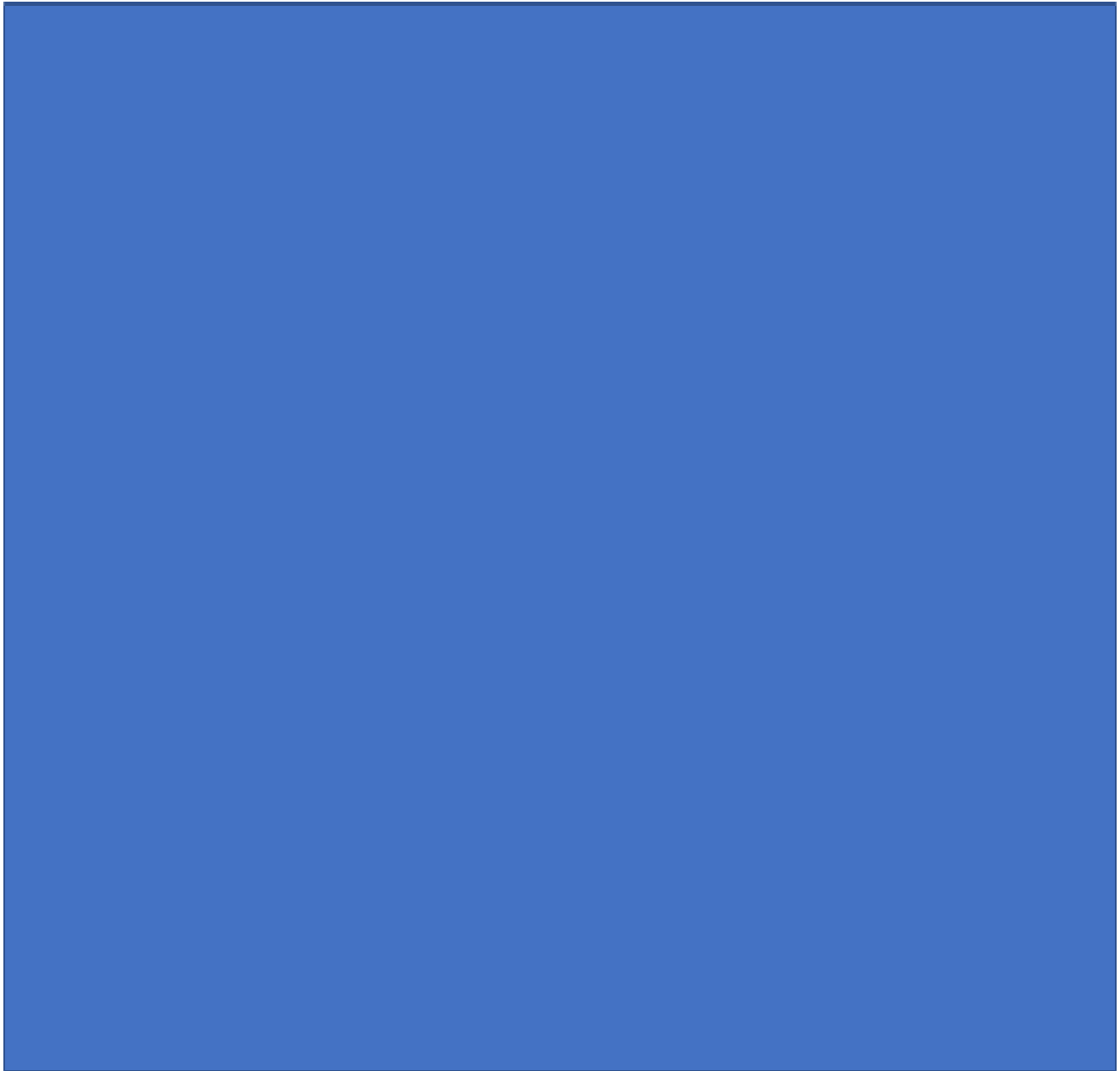
TUCSON UNIFIED
SCHOOL DISTRICT

APPENDIX C

Business Impact Analysis and Infrastructure Upgrade Plan

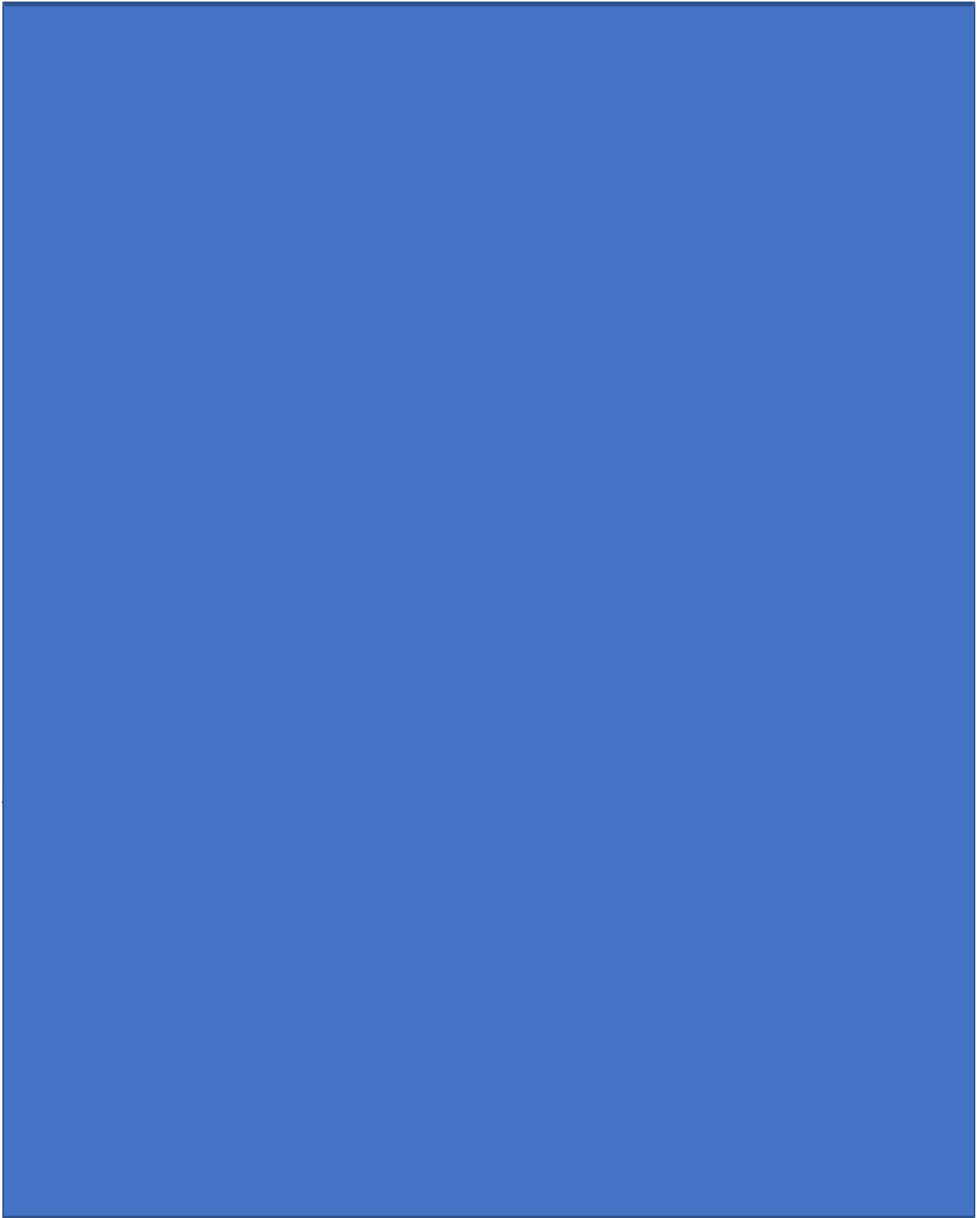
Date: December 2021

Team: TS Infrastructure and Architecture Teams





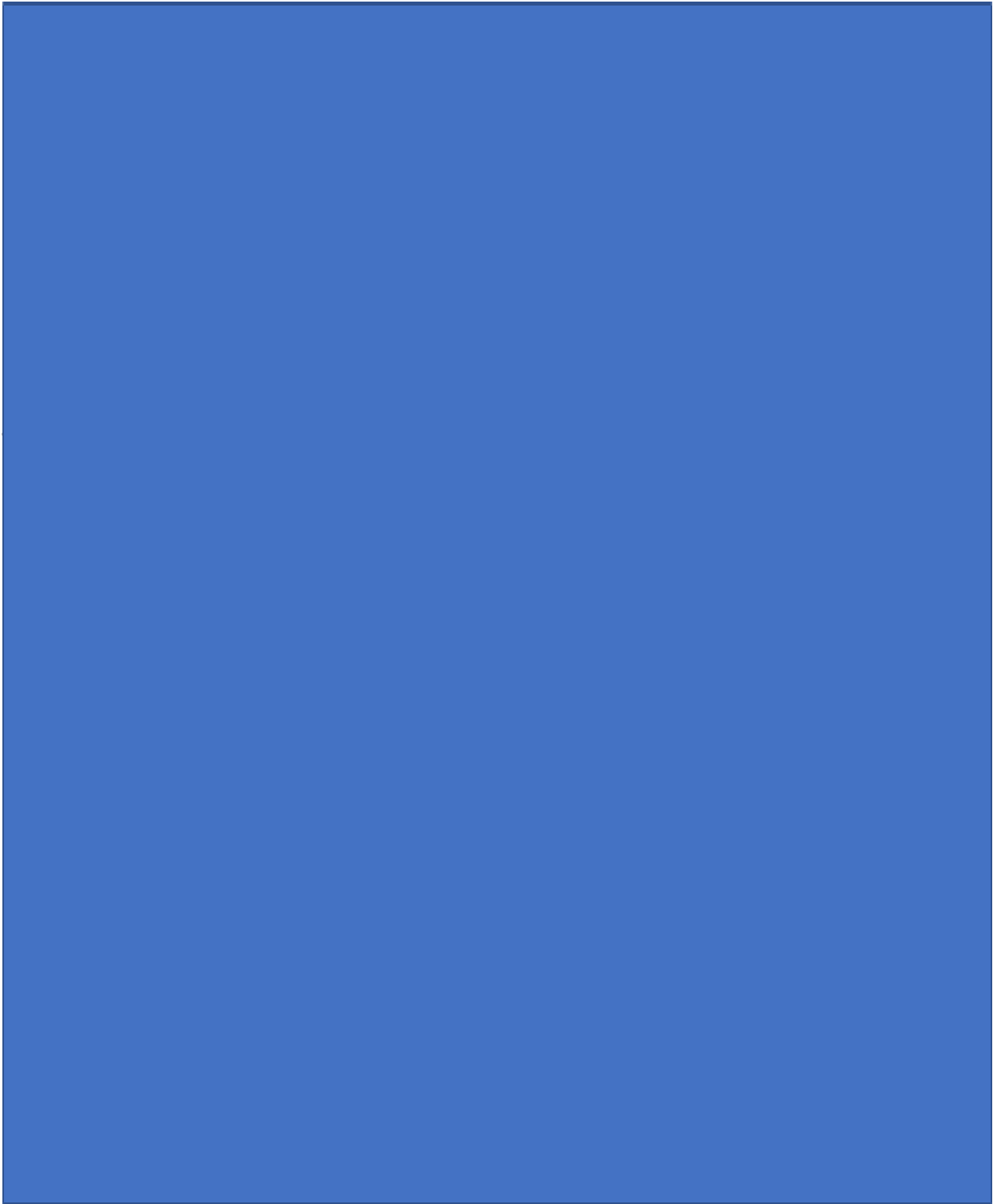
TUCSON UNIFIED
SCHOOL DISTRICT





TUCSON UNIFIED

SCHOOL DISTRICT





TUCSON UNIFIED SCHOOL DISTRICT

APPENDIX D

Standard Operating Procedures for Disaster Recovery & Business Continuity

Date: July 2022

Standard Operating Procedures for Disaster Recovery & Business Continuity

The Technology Services (TS) Department has created a list of standard operating procedures for Disaster Recovery (DR) and Business Continuity (BC).

The list is reviewed and updated regularly by key leaders and personnel on the TS team, and District team when relevant, based on a set timeline (bi-annually) or based on current events or required systems upgrades (for example: COVID events, migration of systems to the cloud, other).

The procedures are based on the information and processes outlined in the Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) provided and adopted by the Technology Services Department.

The list of standard operating procedures for DR & BC includes:

1. **Primary Document:** The DRP & BCP is the primary document adopted and followed by TS, including processes, procedures, tier levels, records, contact information and other relevant information contained in the DRP & BCP
2. **Updates:** THE DRP and BCP document is updated bi-annually and when required based on need, events, changes or upgrades
3. **Meeting Agenda:** DR and BC topics are discussed regularly and as needed during TS department meetings. Plans or changes to procedures are adopted when necessary. Some of the regular meeting include, but are not limited to:
 - a. TS Department Meetings (Monthly)
 - b. TS Department Leadership Meetings (Weekly)
 - c. Change Management Meetings (Weekly)



TUCSON UNIFIED SCHOOL DISTRICT

- d. Architecture Planning and Review Meetings (Bi-Weekly)
 - e. Project Management Meetings (Bi-Weekly)
4. **Data Backup:** Data is backed up daily and weekly on a regular basis and based on needs or events. Back up methods include, but are not limited to: Full, Incremental and Differential methods. Data is restored when needed. System platforms include Physical, Virtual and Cloud
 5. **Systems and Devices:** Systems and Devices are checked, maintained, upgraded and replaced regularly and as needed, based on life cycle and events
 6. **Contracts:** Contracts with Vendors are checked, discussed, edited, upgraded regularly, and replaced when necessary
 7. **Licenses:** Licenses for Systems, Software, Hardware and Applications are reviewed, discussed, upgraded, changes regularly and replaced when necessary
 8. **Communication and Coordination:** Communication to District stakeholders is done regularly during scheduled, or ad hoc, meetings regarding DR and BC topics. Stakeholders include, but are not limited to: School, Site and Department Leaders (Principals, Teachers, Administrators, Directors, Managers, Technicians, Staff); Superintendent and Superintendent Leadership Team (SLT); Governing Board; Audit Committees; Oversight Committees; Unitary Status Plan (USP) legal team; School Safety; Vendors and Contractors; Utility Companies.
 9. **Reports:** Reports are provided regularly and when requested. Reports include, but are not limited to: DR and BC Updates; Unitary Status Plan reports; Technology Condition Index (TCI) Report; Facility Condition Index (FCI) Report; Projects Reports.
 10. **Training:** DR, BC, security (Cyber Security, IT and non IT security) and data recovery training is required and provided regularly to TS and, when necessary, District key personnel. Training methods include, but are not limited to: cross training; in-person training; online Training; vendor/contractor training; college courses; local, state and national conferences and seminars.



TUCSON UNIFIED SCHOOL DISTRICT

APPENDIX E

Policies for Disaster Recovery and Business Continuity

Date: July 2022

Technology Services Policies for Disaster Recovery and Business Continuity

The Technology Services (TS) Department has created and adopted a list of policies, processes and procedures in the Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).

The TS Department will be recommending the adoption of DR and BC policies to the Tucson Unified School District Governing Board during School Year 2022 – 2023 (SY22-23). The recommendations will be discussed initially with relevant district stakeholders, the Superintendent and the Superintendent Leadership Team.

The TS Department will also be recommending and leading, or playing a major role in, a district-wide DRP and BCP during SY22-23, with a target completion date during SY22-23 or SY23-24.

The current DR and BC list of policies and policy-related information included in the DRP and BCP:

1. Full DRP and BCP - Detailed info of policies, processes, procedures
2. Disaster event declaration policy
3. Contact Information for key TS and District personnel
4. Contact Information for key TS and District vendors
5. Recovery Definitions: Recovery Time Objectives (RTO), Recovery Point Objectives (RPO) and Tier Levels
6. Inventory of Systems and Devices (attached *DRBC Device List*)
7. Network Architecture
8. Systems and Devices technical and non-technical information
9. Recovery Procedures and Processes
10. Data centers locations and Information



TUCSON UNIFIED SCHOOL DISTRICT

11. Vital records locations and Information
12. Testing Calendars and Reports (confidential reports provided upon request)

Some current technology policies adopted by the Governing Board are listed and attached. The listed policies play a role in preventing disasters and major incidents that may disturb the district operations and instructions.

1. Policy Code: EJA – Acceptable Use of Technology Resources
2. Policy Code: EJG – Telephone Usage (Desk Phones, Fax Lines, Cell Phones, Radios)
3. Policy Code: IJNDB – Use of technology Resources in Instruction
4. Policy Code: IJNDB-R2– Laptop Usage - Use of Technology Resources in Instruction



TUCSON UNIFIED
SCHOOL DISTRICT

APPENDIX F

Appendix F contains a group of confidential documents.

The documents were provided for this audit upon request.

For security reasons, these documents can be provided only upon request and in an encrypted format for a limited time.

The titles of the documents for purposes of this audit are:

Audit-TS-DRBC-5-BackupLog-PhysicalVirtual1-July2022

Audit-TS-DRBC-5-BackupLog-PhysicalVirtual2-July2022

Audit-TS-DRBC-5-BackupLog-Cloud-July2022

The documents contain approximately 600 data entries of backup logs for Information Technology devices and applications that run the District's operations



TUCSON UNIFIED
SCHOOL DISTRICT

APPENDIX G

Appendix G is a confidential document.

The document was provided for this audit upon request.

For security reasons, this document can be provided only upon request and in an encrypted format for a limited time.

The title of this document for purposes of this audit is:



The document contains the inventory and relevant information for approximately 500 essential Information Technology devices and applications that run the District's operations.



TUCSON UNIFIED
SCHOOL DISTRICT

APPENDIX H

Appendix H is a confidential document.

The document was provided for this audit upon request.

For security reasons, this document can be provided only upon request and in an encrypted format for a limited time.

The title of this document for purposes of this audit is:



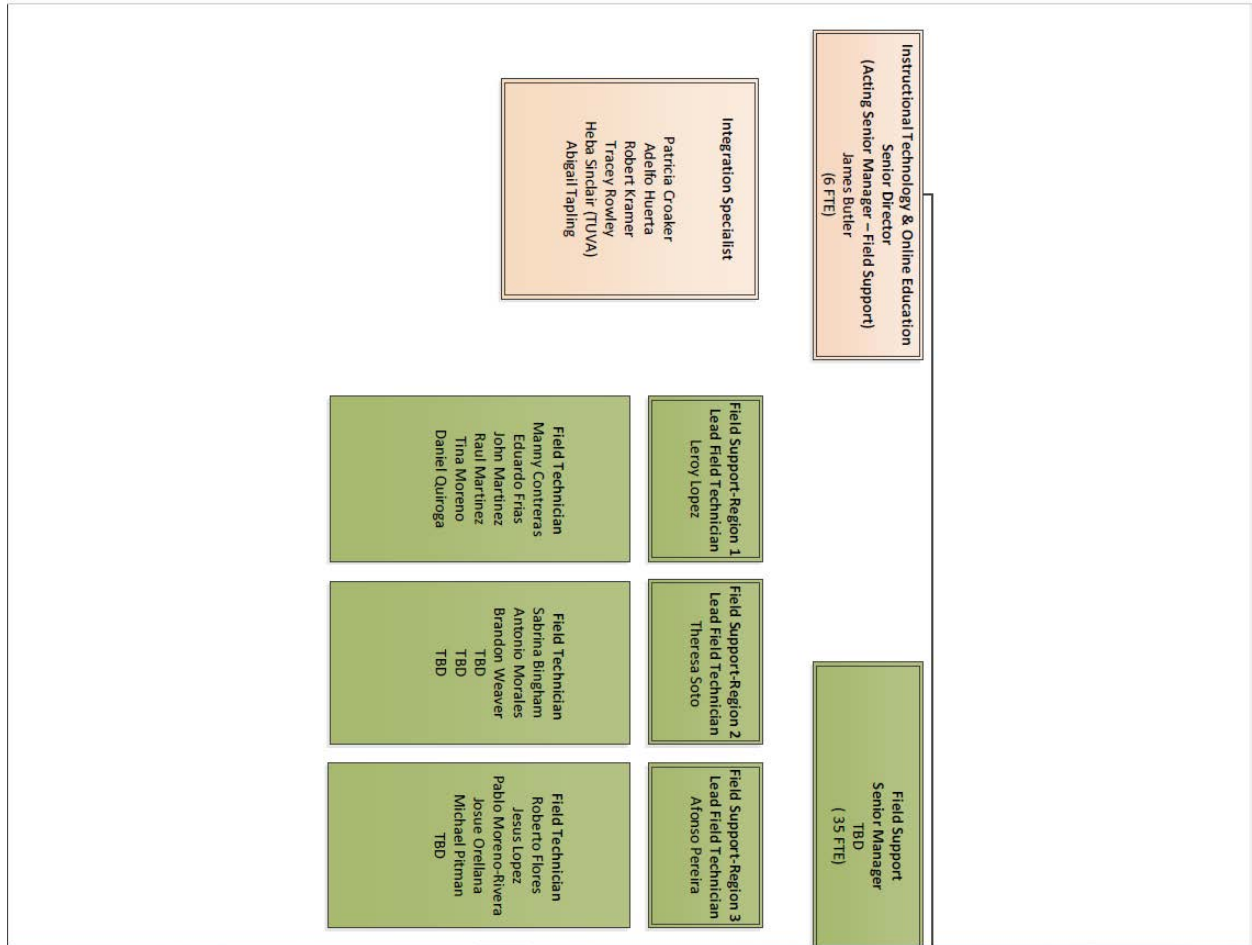
The 100-page document contains test results and information for a security assessment of some of the District's technology systems. The security assessment was performed by a third party.



TUCSON UNIFIED
SCHOOL DISTRICT

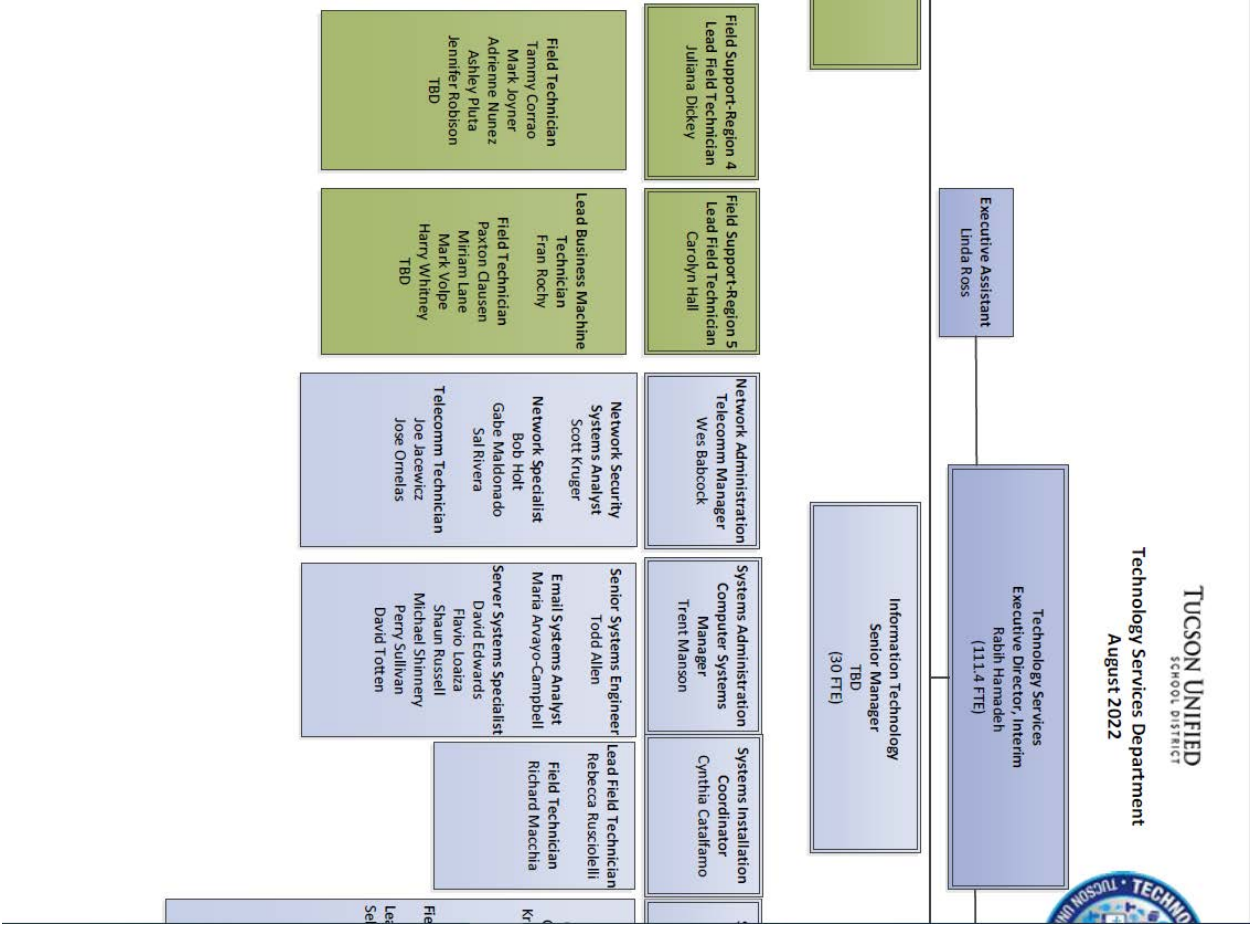
APPENDIX I

Technology Services Organizational Chart – August 2022





TUCSON UNIFIED SCHOOL DISTRICT





TUCSON UNIFIED SCHOOL DISTRICT



Program Analyst
Donna Hankins

App

Service Assurance
Manager
David Rusdolelli

Library And Digital Resources
Program Coordinator
Susan Metzger

Application Services
Program Coordinator
Kimberly Elias

School Office Services
Program Coordinator
Mike Dunn

P

Warehouse Assistant
Susan Smith

MTSS Applications Engineer
Christopher Anderson
Computer Support Training Specialist
Sara Jones
Julie Kossmann
Crystal Mcnair
SIS Systems Analyst
TBD
SIS Application Engineer
Laureen Welborn
Ex Ed Technology Specialist
Christopher Lucas (Ex Ed)

Financial Systems Analyst
Michael Coia
Programmer
Debra Shoemaker
Application Analyst - Office
Manager Mentor
Katy Arvizu
Kimberly Trollden
Roving Staff
TBD (5 x.5 FTE)

Service Desk
Tech Support
Specialist II
Gene Armstrong
Robert Goodman
Ponce de Leon
David Saldate
Barry White

Support-Central
Field Technician
Assistant
Nightsshade
David Yazze

Field Technician
Elias Mitsos
Hayden Smith



TUCSON UNIFIED SCHOOL DISTRICT

Application & Data Services
Senior Manager
Andrew Agnew
(37.4 FTE)

Data Services
PS Programming Mgr. (Act)
Shannon Toms

Senior Programmer
Donna Fine
Teri Reeves (TS, Ex Ed)
TBD
Programmer
Terry Snyder
Senior Data Analyst
Betty Zaenski
Data Analyst
David Scott

School Community Services
Program Coordinator
Kristina Greblocki

Student Services Associate
Belén Gamez
Reyna Vazquez
Myria Rodriguez
Jessica Lopez
Enrollment Coordinator
Leigh Moyor
Denisse Brito
Vanessa Garcia
Maria Lizardo-Gomez
Melissa Stark
Sonia Valencia
Ryan Schmidt

Database Administration
Database Administrator
Rick Foster

Cloud Architecture
Cloud Solutions Architect
Matt Wright



TUCSON UNIFIED
SCHOOL DISTRICT

APPENDIX J

**Responses to the Internal Audit Consultation Report Draft
Topic: Disaster Recovery Plan (DRP)**

Date: June 30, 2021

Prepared by:

Blaine Young, Chief Technology Officer

Rabih Hamadeh, Director of Information Technology Infrastructure

The Technology Services (TS) Department recognizes and appreciates the work done by Ms. Martha Smith, the Internal Auditor for Tucson Unified School District, to complete this audit report. We have discussed the report’s findings and observations with our teams and are providing in this document relevant responses and feedback.

We at the TS department are committed to providing exceptional technology support for our District, and are constantly searching for ways and best practices to improve and update our systems and support models, including Disaster Recovery Plans and Processes.

Responses to the Internal Audit Consultation Report:

1. Technology Department Name – “Information Technology (IT) Department”, cover page (and other pages when used): The correct department name is the Technology Services (TS) Department, not the Information Technology (IT) Department. The Technology Services department includes the Information Technology Team, The Instructional Technology & Online Education Team, and the Application & Data Services Team. The Disaster Recovery Plan (DRP) applies to all three teams within the TS department. A TS Organization Chart was provided.
2. Report Title – “Disaster Recovery and Business Continuity Plan (DRBCP)”, cover page (and other pages when used): The Audit Letter of Intent provided by the Internal Auditor stated that the scope of the audit was the Disaster Recovery Plan (DRP), not the Disaster Recovery and Business Continuity Plan (DRBCP). Business Continuity Planning (BCP) is distinct and separate from Disaster Recovery Planning (DRP) but it does complement it. The BCP involves many aspects of recovering business functions, not just technology,



TUCSON UNIFIED SCHOOL DISTRICT

and needs to be planned and led by the respective departments owning those business functions.

It is important to recognize that the District successfully operated all business functions and instructional delivery in a business continuity mode of operation from March 2020 to March 2021 during the COVID-19 pandemic. Instructional delivery has continued to occur remotely for a large portion of the student population up until the present time. These accomplishments clearly demonstrate that the Technology Services team, district departments and school campuses can and have achieved successful business continuity execution. We do acknowledge that the District has an opportunity to formalize documents for Business Continuity Planning.

3. Overview - Methodology, page 4: Agreed upon Zoom meetings (no physical contact, no in person meetings, no site visitations, etc...) were used due to the COVID-19 pandemic.
4. Observation #1 – “No Departmental Policies and Procedures”, pages 5-6: The TS DRP does self-document when and how the plan is used and when plan updates are made. Other technology policies and procedures are in place, but are beyond the scope of the audit.
5. Observation #2 - “Incomplete Information Technology Disaster Recovery Manual” pages 6-8: A DRP can have many formats and templates. It is not a unique document. What the audit report categorized as incomplete information could be information presented in different formats and contexts, using various tools. When our Technology Services team developed the district DR plan, we collaborated on the content needed to successfully recover the district’s systems. DRP is an important process but we want to point out that our TS team regularly responds successfully to system and network outages on a timely and professional basis. This too is demonstration of an IT organization’s ability to respond to outages of all sizes that impact the organization.
6. Observation #3 – “Vendor Reliability and Support”, pages 8-9: Vendors provide contact information that they deem necessary. TS negotiates and coordinates with vendors as needed in the event of a disaster or for general support, per the contracts. TS has gone through a tiered process that identifies the criticality of systems. Maintenance contracts and support level agreements with vendors are selected based on the critical nature of the systems.
7. Observation #4, “No Information Technology Business Continuity Plan”, page 9: The scope of the audit per the Audit Letter of Intent did not include the Business Continuity Plan (BCP). Please refer to response #2 above.
8. Observation #5 – “No Disaster Recovery for Essential District Departments”, page 10: The following statement extracted in the internal auditor’s report from the DRP overview, “While the District does currently have institutional practices for backup and recovery of district systems, based on a recent audit finding, there is a clear need to formally document a comprehensive approach for Disaster Recovery (DR) of the



TUCSON UNIFIED SCHOOL DISTRICT

District's systems and data", is explaining the reason for the DRP that was developed. The DRP is the formal response to the gap identified by the Arizona Auditor General. This plan was reviewed with the District's Audit Subcommittee in School Year (SY) 18-19.

9. Observation #6, "No Core Principles, References, or Criteria", pages 10-11: The DRP is not a unique document. The DRP may have different formats as determined by a given organization. The tiering of systems, and associated Recovery Point Objectives (RPO), and Recovery Time Objectives (RTO) are clearly stated for District's systems, and are included in the DR Plan and DR Records (Appendix A – Excel List) as criteria.
10. Observation #7, "Providing Information Beyond the Scope of the Audit", page 11: Information was provided per request and was intended to answer the questions in a comprehensive manner. Some relevant information may be included with other data in larger documents. For example, requested vendor contracts were submitted in full rather than extracts. Approximately 400 documents were provided for the internal audit, out of approximately 600 documents that were prepared by TS.
11. Observation #8, "Incomplete Documentation of Disaster Recovery Testing", page 11-13: Relevant testing documentation was provided. Testing documentation and information may have multiple formats. Additional requested documents and answers were provided as discussed in follow up meetings, when requested.
12. Observation #9, "Information in the Business Impact Analysis (BIA) Contains Errors", page 13-15: Typos or blanks will be corrected as needed. Some blank cells or N/A are per design. The indicated example of the "1819" school year was meant to be the 18-19 school year. The indicated "Type" example has a sub-heading titled: Hostname – All Physical that clarifies the type in the list.
13. Observation #10, "Oversight in the Information Technology Disaster Recovery Plan", pages 15-16: Typos will be corrected as needed. DR document formats are not unique, and may have multiple forms. Acronyms definition are optional and may be used based on type of documents, intended audiences and other factors. Original dates indicated in tables are projected, while updated dates are exact.