|  |
| --- |
| Nogales Unified School District #1 |
| Information Technology Policies and Procedures |



**Information Technology Department**

**Name Here**

Information Technology Director

(520) XXX-XXXX

|  |  |
| --- | --- |
| **Name Here** | **Name Here** |
| District Network Technician | District Computer Technician |
| (520) XXX-XXXX | (520) XXX-XXXX |
|  |  |
| **Name Here** | **Name Here** |
| District Computer Technician | District Computer Technician |
| (520) XXX-XXXX | (520) XXX-XXX |

[General Introduction 6](#_Toc514674273)

[Hardware Standards 7](#_Toc514674274)

[1.1 New Desktop and Laptop Workstations 7](#_Toc514674275)

[1.2 Legacy Desktop and Laptop Workstations 8](#_Toc514674276)

[1.3 Printers 9](#_Toc514674277)

[1.4 Cabling Standards 10](#_Toc514674278)

[1.5 Hardware Review and Adoption Process 13](#_Toc514674279)

[1.6 Software Review and Adoption Process 13](#_Toc514674280)

[Software Standards 16](#_Toc514674281)

[1.7 Supported Administrative Software 16](#_Toc514674282)

[1.8 Supported Instructional Software 16](#_Toc514674283)

[1.9 Supported Data Center Software 16](#_Toc514674284)

[1.10 Approved/Unsupported Software 17](#_Toc514674285)

[1.11 Restricted Software 17](#_Toc514674286)

[1.12 Software Revision Control 18](#_Toc514674287)

[1.13 Anti-Virus and Malware Protection 19](#_Toc514674288)

[Initiating Work orders 20](#_Toc514674289)

[1.14 Malfunctioning Hardware or Software 20](#_Toc514674290)

[1.15 Requests for Moves, Adds, Changes, or Other Services 20](#_Toc514674291)

[1.16 Emergency Work orders 20](#_Toc514674292)

[Use of Technology and Security 21](#_Toc514674293)

[1.17 Internet Use Policies 21](#_Toc514674294)

[1.18 Wireless Networking and Access 30](#_Toc514674295)

[1.19 Password Requirements and Change Policy 32](#_Toc514674296)

[1.20 Employee User Account Creation 33](#_Toc514674297)

[1.21 Employee Termination and Process for removing employees from the network 33](#_Toc514674298)

[1.22 Physical Security 33](#_Toc514674299)

[IT Contingency Plan 35](#_Toc514674300)

[1.23 PURPOSE 36](#_Toc514674301)

[1.24 SCOPE 36](#_Toc514674302)

[1.25 PLAN INFORMATION 36](#_Toc514674303)

[CONTINGENCY PLAN OVERVIEW 38](#_Toc514674304)

[1.26 OBJECTIVES 38](#_Toc514674305)

[1.27 ORGANIZATION 38](#_Toc514674306)

[1.28 CONTINGENCY PHASES 41](#_Toc514674307)

[1.29 ASSUMPTIONS 42](#_Toc514674308)

[1.30 CRITICAL SUCCESS FACTORS AND ISSUES 42](#_Toc514674309)

[1.31 MISSION CRITICAL SYSTEMS/APPLICATIONS/SERVICES 43](#_Toc514674310)

[1.32 THREATS 43](#_Toc514674311)

[SYSTEM DESCRIPTION 45](#_Toc514674312)

[1.33 PHYSICAL ENVIRONMENT 45](#_Toc514674313)

[1.34 TECHNICAL ENVIRONMENT 46](#_Toc514674314)

[PLAN 48](#_Toc514674315)

[1.35 PLAN MANAGEMENT 48](#_Toc514674316)

[1.36 TEAMS 49](#_Toc514674317)

[1.37 DATA COMMUNICATIONS 53](#_Toc514674318)

[1.38 BACKUPS 53](#_Toc514674319)

[1.39 Restoration Policy 53](#_Toc514674320)

[1.40 VITAL RECORDS/DOCUMENTATION 53](#_Toc514674321)

[1.41 OFFICE EQUIPMENT, FURNITURE AND SUPPLIES 54](#_Toc514674322)

[1.42 RECOMMENDED TESTING PROCEDURES 54](#_Toc514674323)

[Logging and monitoring audit policy 56](#_Toc514674324)

[Controlling administrative access/rights 57](#_Toc514674325)

[APPENDICES 59](#_Toc514674326)

[A. CONTINGENCY PLAN CONTACT INFORMATION 60](#_Toc514674327)

[B. EMERGENCY PROCEDURES 62](#_Toc514674328)

[C. SOFTWARE INVENTORY 65](#_Toc514674329)

[D. HARDWARE INVENTORY 66](#_Toc514674330)

[E. COMMUNICATIONS REQUIREMENTS 68](#_Toc514674331)

[F. EXTERNAL SUPPORT AGREEMENTS 69](#_Toc514674332)

[G. DATA CENTER EMERGENCY PROCEDURES AND REQUIREMENTS 70](#_Toc514674333)

[H. PLAN MAINTENANCE PROCEDURES 72](#_Toc514674334)

[I. CONTINGENCY LOG 73](#_Toc514674335)

[J. NUSD Information Technology Services Log Monitoring 75](#_Toc514674336)

K. Safety Guidelines for Power Strip and Extension Cord Use SOP……………………………………78

# General Introduction

This document contains the current standards and procedures by which the Information Technology Department functions and the policies that support the acquisition and support of technology in the Nogales Unified School District.

These standards exist as a guideline to assist the staff of Nogales Unified School District in the effective purchase, use, and maintenance of technology in order to support the staff in our common goal of providing the best education possible for the students of Nogales Unified School District.

# Hardware Standards

The minimum standard hardware configurations for all student, teacher, and administrative workstations described within this document are required to be eligible for District support. District support includes, but is not limited to:

* District provided installation and setup services
* Connectivity to the district network
* District provided software installation and support
* District provided repair services

Described configurations constitute minimum standards, except where indicated, and are subject to periodic revision.

All new workstation and laptop purchases must be must be compliant with these specifications, and must be made through the District Purchasing Department and approved by the Information Technology Director.

**Donated Equipment:** In general, the District will not support any donated desktop or laptop workstations not meeting minimum standards. Donated workstations believed to meet or exceed minimum district standards must be inspected by a Computer Technician prior to that machine being placed into service.

* New workstations purchased using donated funds that meet the minimum standards **will be** supported by the district, and will be eligible to be connected to the district network.
* Computers provided through refurbishment programs are not eligible for district support.
* All donated workstations or other workstations purchased that do not comply with these standards will be permanently tagged as unsupported hardware.

By directive of the Superintendent of Schools, there will be NO EXCEPTIONS to these policies.

## New Desktop and Laptop Workstations

**PC Desktop Standards**

All standards are minimums unless an exception is explicitly stated. Specific makes and models of components shall be purchased where noted.

| Description | Standard |
| --- | --- |
| Processor | 3.2 GHz  |
| RAM | 8 GB |
| System Drive (SSD preferably) | 256 GB  |
| Network Interface Card | 1 Gbps |
| Wireless Network Interface Card | 802.11n |
| Video RAM | 1 GB |
| Optical Drive | 16x DVD +/-RW |
| Display Size | 23” LCD 1920 x 1080 |

**Laptop Standards**

All standards are minimums unless an exception is explicitly stated. Specific makes and models of components shall be purchased where noted.

|  |  |
| --- | --- |
| Description | Standard |
| Processor | 3.2 GHz  |
| RAM | 8 GB |
| Sytem Drive (SSD preferably) | 256 GB  |
| Network Interface Card | 1 Gbps |
| Wireless Network Interface Card | 802.11n |
| Video RAM | 1 Gigabit |
| Optical Drive | 16x DVD +/-RW |
| Display Size | 13” LCD |

## Legacy Desktop and Laptop Workstations

**PC Desktop Standards**

The district will not support legacy desktop due to incompatibility to curriculum and instruction needs.

All standards are minimums unless an exception is explicitly stated. Specific makes and models of components shall be purchased where noted.

|  |  |
| --- | --- |
| Description | Standard |
|  |  |
|  |  |
|  |  |
|  |  |

**Laptop Standards**

The district will not support legacy desktop due to incompatibility to curriculum and instruction needs.

All standards are minimums unless an exception is explicitly stated. Specific makes and models of components shall be purchased where noted.

|  |  |
| --- | --- |
| Description | Standard |
|  |  |
|  |  |
|  |  |
|  |  |

## Printers

These configurations and standards are subject to periodic revision based upon evolving technology and availability of equipment.

Eligibility for District support requires all new printer purchases to be made through the District Purchasing Department and approved by the Information Technology Director, and be in compliance with these specifications. Only those models currently available on District bid or State Contract that have been tested and approved by Information Technology will be supported.

**Ink Jet Printers**. Ink Jet printers may be purchased and connected directly to a workstation as a slave printer only. Due to the low cost of these printers and the high cost of repair and operation, these printers are classified as “consumable hardware.” The district cannot bear the high cost of repair and maintenance of such printers and therefore will not repair them. The campus or department shall be responsible for the repair or replacement of said equipment.

**Donated Hardware**. The district will NOT support any used donated printers. Donated printers include printers provided through refurbishment programs. New printers purchased using donated funds that meet the minimum standards WILL BE supported by the district, and will be eligible to be connected to the district network or district workstations as applicable.

All donated printers or other printers purchased not in compliance with these standards will be permanently tagged as unsupported hardware.

By directive of the Superintendent of Schools, there will be NO EXCEPTIONS to these policies.

**Approved Printer List**

| Description | Model |
| --- | --- |
| Laser, Black/White, Workgroup | HP, Ricoh, Lanier, Dell |
| Laser, Color, Workgroup | HP, Ricoh, Lanier, Dell |
|  |  |
|  |  |

## Cabling Standards

**General Cabling**

* All network drops will be a minimum of Category 6 rated cable with plenum jackets. New construction and major renovations will receive a minimum of two Category 6 cables to each administrative or general-purpose faceplate. Any classroom defined as a general-purpose room shall receive a minimum of six Category 6 cables located throughout the room unless otherwise specified. Other configurations will be defined as needed. This configuration will support current applications and present an additional growth capability.
* All voice drops will be a minimum of a single drop of Category 6 rated cable with plenum jackets. New construction and major renovations will receive one Category 6 cable to each administrative or general-purpose faceplate. Other configurations will be defined as needed. This configuration will support current applications and present an additional growth capability.
* The network drops will be terminated in compliance with Category 6 specifications and labeled in an acceptable manner.
* All cable that runs back to cable telecommunications closets will be terminated on a Category 6 rated patch panel and labeled in a manner deemed acceptable
* The cabling contractor will provide cable certification reports and warranty statements to verify each Category 6 drop.
* Copper/UTP Category 6 cable runs exceeding 295 feet will be deemed unacceptable, as they would be out of specification with regard to the EIA/TIA 568A specification. (This situation identifies a need for an additional IDF location, which would link back to the MDF via fiber-optic cabling.)
* All network drops will be terminated in a 568-B configuration.

**Horizontal Cabling**

* The maximum permitted horizontal distance is 90 meters (295'), which will allow 10 meters (33') for patch cables, jumper cords, etc. (Total combined maximum length not to exceed 100 meters).
* The horizontal cable manufacture must be approved by the Information Technology Department.
* Copper cabling must have all four pairs terminated and pairs must not be split between jacks. Exceptions to this may arise and will be at the discretion of the Information Technology Department. The Exceptions must be approved by the Information Technology Department during the planning phase and included in the construction drawings and documents and in the scope of work for the cabling contractor.

**Backbone Cabling** (Feeders and Risers)

This section will be determined by the specific requirements of the project and approved by the Information Technology Department on a case-by-case basis.

**Equipment Room**

All Cable closets (IDFs) with fiber runs will have a minimum of one six-strand, 62.5 micron multi-mode fiber and one six-strand single-mode fiber run back to the MDF. Twisted pair copper riser may be requested with the pair count determined on each project. Other fiber optic strand counts may be specified as needed.

**Exterior Cabling**

All exterior cabling must adhere to AIAA Standards or Local Area Best Practices. This section will be determined by the specific requirements of the project and approved by the Information Technology Department on a case-by-case basis. The installation of cabling over a building’s exterior roof is expressly forbidden.

**Fiber Cabling**

* All fiber strands will be terminated with SC connectors unless otherwise specified.
* All Cable closets (IDFs) with fiber runs will have one six-strand, 62.5 micron; multi-mode, fiber, and one six-strand single-mode fiber run back to the MDF. Additional strand count may be specified as needed.
* Fiber runs will be protected in plenum rated inner ducts.
* Fiber runs at any location will start from the Main Distribution Frame (MDF) centrally located in the building and going out to Intermediate Distribution Frames (IDFs) throughout the location.
* All fiber optic cable and fiber termination equipment and products will be approved by the Information Technology Department via a formal submittal.

**Copper Cable Installation Requirements**

* Category 6 Plenum rated cables will be installed for all interior environments. The cable manufacturer product(s) must be presented to the Information Technology Department and deemed acceptable for use prior to installation.
* All patch and station cables will be terminated on Category 6 rated RJ45 jacks.
* All patch and station cables will be kept to a minimum length in order to keep the channel distance within the 100-meter specification, as set by the EIA/TIA.
* Patch cables shall be installed to the top switch first and be fully populated before installing to the next switch. Patch cables shall not cross one another vertically or horizontally when transitioning from cable management to the switch.
* Patch cables shall not cross one another vertically or horizontally when transitioning from cable management to the patch panel.
* All data cable installations will meet or exceed Category 6 Standards from the originating IDF to the furthest remote cable termination point.

**Fiber Optic Cable Installation Requirements**

* Entire cable runs will be installed in one continuous length from bulkhead connector to bulkhead connector, including coiled loops, without splices or repairs.
* All fiber distribution panels will have plastic dust caps on each unused fiber termination.
* Multi-mode fiber patch cables will be terminated with ‘SC’ connectors on one end and as required on the other end unless otherwise specified.
* Single-mode fiber patch cables will be terminates with “SC” connectors on one end and as required on the other end unless otherwise specified.
* Bulkhead distribution cabinets must have labels showing cable numbers and far end location for each cable terminated in the cabinet.
* Aerial installation of fiber optic cable is prohibited unless written approval is received from the District.
* Cable installation shall meet all manufacturer specifications for tensile strength; bend radius, and vertical rise. All pulls involving a winch must be monitored for tension and cannot exceed the maximum tensile rating.
* Lubricants may be used to facilitate pulling of cables but the lubricant must not be harmful to the cable, the raceway or humans.
* Each time a cable enters a cabinet or junction box it must be securely tied down with cable ties.
* No individual exposed fibers will be permitted.
* Cable entrances into equipment or cabinets must be protected with insulated bushings or grommets.
* A minimum of ten feet of extra cable should be coiled as a service loop at each end of each run.
* Each end of the fiber optic cable shall be labeled specifying the far end building name, building number, single-mode or multi-mode, and the strand count. The cable shall be also be labeled on each end at the point the cable leaves the tunnel system if it enters a conduit. The label shall be placed between 12 inches and 36 inched from the conduit or at the closest point that it is clearly visible. Termination panels at both ends shall be labeled with the far end building name, building number, single-mode or multi-mode, and the strand count.

## Hardware Review and Adoption Process

The requestor must provide a business case as to why a particular piece of equipment, other than one on the current standards list, is necessary. A statement of functionality over and above a currently approved piece of equipment must be included as part of the business case. Excess budget is not a sufficient business reason for modification of these standards.

A vendor must be willing to provide a requested piece of equipment to the district, at no cost to the district, for a period of not less than one month for testing purposes. The requested piece of equipment shall be installed and configured by Information Technology Department personnel at the site of the requestor. The requestor shall use the requested product as part of normal business operations for a period of not less than one month. The requestor shall submit, via e-mail, a written evaluation of the requested product to the Information Technology Director highlighting the assets and deficiencies of the product being evaluated. The Technician who installed the requested product at the requestor’s site shall submit, via e-mail, a written report to the Information Technology Director regarding the installation, configuration, and removal of the product.

The Information Technology Director will determine, based upon the information received and any other pertinent information, whether or not the product shall be added to the District Standards.

## Software Review and Adoption Process

**Software Review and Adoption Participants**

An ad-hoc Software Review/Adoption Committee will be formed to review requests to acquire new software that is not already on an approved software list. This committee will be responsible for reviewing these requests and submitting a recommendation of approval or rejection to the Information Technology Director.

The Committee should consist of appropriate membership, which may include any of the following positions: an administrator from the school or department initiating the request, an Instructional Technology Specialist or Support Associate, a curriculum resource coordinator in the discipline affected.

The objective of Software Review and Adoption Committee is to:

* Ensure that the instructional content aligns with district teaching objectives and standards.
* Ensure that proposed software systems will operate on existing hardware platforms; and if not, to determine what upgrades will be required to accommodate the proposed software systems.
* Ensure that proposed software systems will operate on existing operating systems.
* Ensure that proposed software systems will operate on existing network infrastructure.
* Ensure that proposed software systems will not subject the district to security risk.
* Help prevent unexpected effects on existing hardware and software systems.
* Eliminate redundant or conflicting software systems.

**Resources Required**

A test environment will be established and maintained with current supported workstation, server, software, and networking environments in order to perform the following tasks associated with software review:

* Conduct the Compatibility and Requirements Reviews
* Conduct the Performance Tests
* Complete Reports on findings
* Research new hardware and software
* Maintain and publish the Software Status Lists

A test environment should include the following minimum requirements:

* A server for each supported platform
* A workstation for each supported environment
* An isolated secure network

**Software Review and Adoption Process**

A Software Review and Adoption Committee will be convened and scheduled upon the submittal of a request for software review and adoption. The review and adoption procedure is as follows:

1. The requesting administrator submits a request for software review. The submittal must provide the following information:
	1. Expected Instructional impact and outcomes
	2. Vendor contact information
	3. Desired/Required Implementation: District-wide, school only, department
	4. Expected cost of software or hosted subscription services
	5. Platform: PC, Apple, server based (include platform choices), Web based
	6. Any vendor required hardware
	7. Printing Requirements: frequency and volume
	8. Services to be provided by vendor: installation, training, continuing support
	9. Availability of a minimum 30 day evaluation copy
2. The software is reviewed for instructional merit. **This will require up to 5 working days to complete.**
3. The software is reviewed for compatibility and requirements. An evaluation copy will be required, or a test system made available for hosted systems. **This will require up to 10 working days to complete,** and result in a Compatibility and Requirements Report containing the following information:
	1. Workstations Requirements: minimum hardware specifications, minimum OS level.
	2. Sever Requirements: requires new server, use existing servers.
	3. Network Requirements: impact on bandwidth (LAN/WAN), impact on network security.
	4. Internet Browser Requirements: minimum browser level, required “plug-ins.”
	5. Expected other impacts and required upgrades.
	6. Device requirements encountered.
	7. Verification of workstation performance.
	8. Verification of compatibility with other existing software systems.
	9. Internet security/filtering requirements encountered.
	10. Preliminary Implementation Plan: expected length of time needed to accomplish upgrades and installation, timeframe when resources are expected to be available.

The Compatibility and Requirements Report is submitted to the Information Technology Director with a recommendation for adoption or rejection. If the recommendation is adoption, the software title is then added to either the Approved/Supported List or the Approved/Not Supported List. If the recommendation is for rejection, the software title is placed on the Restricted List with the reasons for rejection.

# Software Standards

## Supported Administrative Software

|  |  |
| --- | --- |
| Description | Title and Version |
| Operating System | 32 or 64-Bit Windows 10 Professional/Education |
| Productivity Suite | Microsoft Office Professional Plus 2016 + |
| Internet Browser | Internet Explorer, Google Chrome, MS Edge, Firefox, Safari |
| Java Runtime Environment | Sun Java Update current version |
| PDF Reader | Adobe Acrobat Update current version |
| Transportation | N/A |
| Library Systems | Follet |
| Food Service | N/A |
| Business  | Visions |

## Supported Instructional Software

Any software compatible with Google Chrome OS, Apple OS, and Windows OS will be supported by the district following the minimum computer specification mentioned in section 1.1.

## Supported Data Center Software

| Description | Title and Version |
| --- | --- |
| Server OS | Microsoft Server 2012 and above |
| SQL | Microsoft SQL Server 2016 and above |
|  |  |
|  |  |

## Approved/Unsupported Software

|  |  |
| --- | --- |
| Description | Title and Version |
|  |  |
|  |  |
|  |  |

## Restricted Software

|  |  |
| --- | --- |
| Description | Title and Version |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Software Revision Control

This section pertains to the testing and implementation of updates and revisions to current standardized software. In order to reduce risk, new versions of software and operating systems will be tested for some period of time before being introduced into the production environment.

The Information Technology Department will maintain a test environment (possibly virtual) comprised of current hardware and desktop configurations. When considering an update or patch to software in the existing environment IT will perform a series of initial tests in this lab environment, then pilot testing before rolling out district-wide as a whole or in a phased approach, depending on the application. This process may require 10 days to 6 months to complete.

**Testing**

* Installation tests – validate installation of the update without error
* Verification tests – verify that shortcuts, help files and file associations are working properly
* Execution tests –verify execution by non-administrator level users
* Standard tests – verify that installation of update does not negatively impact another application found on the desktop or network
* Rollback tests – verify safe method of uninstalling the patch/update and restoring the target system to the pre-patch state

**Pilot Testing**

* A pilot group will be identified based on the type of software, ultimate user population and technical ability required
* The pilot group will perform the required testing scripts and use the software in the normal course of business
* A rollout plan is developed based upon observations during the testing and pilot phases

**Remediation/Rollout**

* Notify affected users in advance of impending change, with instructions as necessary.
* Determine any training requirements and schedule end user training.
* Perform backup of impacted systems as needed prior to deployment.
* Use a phased approach whenever possible. Provide enough time between phases to identify issues before next phased deployment begins.
* Employ policy based remediation for smaller or more critical updates. Monitor network resources during deployment.

In general, district IT will support up to 1 major revision of each application, or versions released within last 12 months, whichever is greater. Software applications of versions older than 12 months will be updated to current supported versions as soon as feasible.

## Anti-Virus and Malware Protection

The district currently employs **Sophos MTR Endpoint Protection** on each Windows Desktop, Laptop computer and Servers.

This enterprise-scale solution provides client management, virus and malware detection, prevention and removal to each computer in the district. Regular definition updates are pushed to each workstation every 8 hours on a staggered schedule. Critical updates are pushed immediately.

All external media, i.e. thumb drives, DVDs, etc., are scanned for malware upon insertion and as files are accessed.

Non-administrators are prohibited by Microsoft App Locker using Group Policy from installing personal or unapproved software. If necessary the software review process must be followed before installation is allowed.

# Initiating Work orders

## Malfunctioning Hardware or Software

The Information Technology Department requires work orders

* To identify chronic problems within families of equipment or software
* To track the movement of equipment in and out of our repair facility
* To document the use of stock parts or outside services that may be used to repair the equipment
* To accumulate repair history on a particular piece of equipment

To file a work order, you will be required to provide certain minimum information such as, the bar code on the equipment affected, and as detailed a description as possible of the symptoms being experienced; including exact text of any error messages being displayed. Requests for work orders will not be accepted without this minimum information.

## Requests for Moves, Adds, Changes, or Other Services

Notify the Computer Technician or school office of the request.

The Computer Technician or school secretary must ensure that the request is approved and funded (if there is a cost involved) before a work order is requisitioned.

Services of this nature include, but are not limited to:

* Requests for additional cable drops for computers or phones
* Requests for installation of Internet connectivity
* Requests for installation of new computers and/or phones
* Requests for existing computers to be connected to the District Network

## Emergency Work orders

A work order shall be classified as an “Emergency” only if one of the following criteria exists:

* **Site Down** - means no one on the site can work because a file server is down or inaccessible because of a hardware or software problem on the network
* **Office/Workgroup Down** – no one in a department or a school office can work
* **Administrative Networked Printer Down** - an entire office/workgroup cannot get printed output
* **Administrative workstation down** - the person cannot do their job and there is no alternative computer available
* **Instructional Lab Down** – All workstations in an instructional lab are down or cannot access needed resources

Work orders not meeting the above criteria and not approved as exceptions shall be placed on normal route status and the appropriate contact person shall be notified.

# Use of Technology and Security

## Internet Use Policies

The documents on the following pages outline the district’s Internet and technology use policies. These agreements must be signed by each student and parent at the beginning of each school year.

Employees must sign the Agreement upon employment.

Attached:

* Staff Use of Digital Communications and Electronic Devices
* Use of Technology Resources in Instruction Policy
* Electronic Information Services User Agreement

**G-1200 © GBEF**

**STAFF USE OF DIGITAL COMMUNICATIONS**

**AND ELECTRONIC DEVICES**

Social media is the use of web-based and mobile technologies to communicate through interactive dialogue. Social media technologies include but are not limited, to blogs, picture-sharing, vlogs, wall-postings, e-mail, instant messaging, music-sharing, crowdsourcing, voice over IP (VoIP), Facebook, LinkedIn, My Space, Twitter, You Tube, and any successor protocol to transmit information. Mobile technologies are any devices that: transmit sounds, images, texts, messages, videos, or electronic information; electronically records, plays, or stores information; or accesses the Internet, or private communication or information networks. Current examples are Smartphones such as BlackBerry, Android, iPhone, and other such mobile technologies and subsequent generations of these and related devices.

The Governing Board recognizes how web-based and mobile technologies are fundamentally changing opportunities to communicate with individuals or groups and how their use can empower the user and enhance discourse. The Board equally recognizes that the misuse of such technologies can be potentially damaging to the District, employees, students and the community. Accordingly, the Governing Board requires all employees to adhere to adopted policies and to utilize digital communications and electronic devices in a professional manner at all times.

The Board establishes the following parameters:

*District employees*

* Shall adhere to all Governing Board policies related to technologies including but not limited to the use of District technology, copyright laws, student rights, parent rights, the Family Educational Rights and Privacy Act (FERPA), staff ethics, and staff-student relations;
* Are responsible for the content of their posting on any form of technology through any form of communication;
* Shall only use District controlled and approved technologies when communicating with students or parents;
* Shall ensure that technologies used to communicate with students and District staff are maintained separate from personal technologies used to communicate with others;
* Shall not use District owned or provided technologies to endorse or promote a product, a cause or a political position or candidate;
* In all instances must be aware of his/her association with the District and ensure the related content of any posting is consistent with how they wish to present themselves to colleagues, community members, parents and students;
* Shall not use District logos or District intellectual property without the written approval of the Superintendent;
* Shall use technologies to enhance and add value to communications with all recipients and be respectful of those with whom they communicate;
* Shall immediately report all misuse or suspected misuse of technology to their direct supervisor/administrator who in turn will immediately report to the Superintendent;
* Shall comply with all applicable records management parameters established by Arizona State Library, Archives and Public Records.

The Superintendent shall communicate the above to all employees of the District at the beginning of each school year and to newly hired employees as part of the hiring process.

The Superintendent shall establish which technologies are approved for use by employees to communicate with parents and students. Approved technologies shall be communicated to the Board and employees prior to the start of every school year, to newly elected Board members prior to taking office, and to newly hired employees as part of the hiring process.

The Superintendent shall determine which records retention and management guidelines as established by the Arizona State Library, Archives and Public Records are applicable to this Board policy and communicate these guidelines to the Board and employees prior to the start of every school year, to newly elected Board members prior to taking office, and newly hired employees as part of the hiring process.

Violations of this policy may result in disciplinary action up to and including termination and may constitute a violation of federal or state law in which case appropriate law enforcement shall be notified. The Superintendent shall report violations of this policy to the Board and shall make reports to the appropriate law enforcement agency when determined necessary.

Adopted: date of Manual adoption

LEGAL REF.: A.R.S. 15-341

 15-514

CROSS REF.: GBEA - Staff Ethics

 GBEB - Staff Conduct

 GBEBB - Staff Conduct with Students

 GCQF - Discipline, Suspension, and Dismissal of

 Professional Staff Members

 GDQD - Discipline, Suspension, and Dismissal of

 Support Staff Members

 IJNDB - Use of Technology Resources in Instruction

 JIC - Student Conduct

**I-6400 © IJNDB**

**USE OF TECHNOLOGY RESOURCES**

**IN INSTRUCTION**

**Appropriate use of Electronic Information Services**

The District may provide electronic information services (EIS) to qualified students, teachers, and other personnel who attend or who are employed by the District. Electronic information services include networks (e.g., LAN, WAN, Internet), databases, and any computer-accessible source of information, whether from hard drives, tapes, compact disks (CDs), floppy disks, or other electronic sources. The use of the services shall be in support of education, research, and the educational goals of the District. To assure that the EIS is used in an appropriate manner and for the educational purposes intended, the District will require anyone who uses the EIS to follow its guidelines and procedures for appropriate use. Anyone who misuses, abuses, or chooses not to follow the EIS guidelines and procedures will be denied access to the District's EIS and may be subject to disciplinary and/or legal action.

The Superintendent shall determine steps, including the use of an Internet filtering mechanism that must be taken to promote the safety and security of the use of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Technology protection measures shall protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography or, with respect to use of computers by minors, harmful to minors. Safety and security mechanisms shall include online monitoring activities.

As required by the Children's Internet Protection Act, the prevention of inappropriate network usage includes unauthorized access, including "hacking," and other unlawful activities; unauthorized disclosure, use and dissemination of personal identification information regarding minors.

It is the policy of the Board to:

* Prevent user access over the District's computer network, or transmissions of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
* Prevent unauthorized access and other unlawful online activity;
* Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
* Comply with the Children's Internet Protection Act [P.L. No. 106-554 and 47 U.S.C. 254(h)].

Each user will be required to sign an EIS user's agreement. The District may log the use of all systems and monitor all system utilization. Accounts may be closed and files may be deleted at any time. The District is not responsible for any service interruptions, changes, or consequences. The District reserves the right to establish rules and regulations as necessary for the efficient operation of the electronic information services.

The District does not assume liability for information retrieved via EIS, nor does it assume any liability for any information lost, damaged, or unavailable due to technical or other difficulties.

**Filtering and Internet Safety**

As required by the Children's Internet Protection Act, the District shall provide for technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by students, harmful to students. The protective measures shall also include monitoring the online activities of students.

Limits, controls, and prohibitions shall be placed on student:

* Access to inappropriate matter.
* Safety and security in direct electronic communications.
* Unauthorized online access or activities.
* Unauthorized disclosure, use and dissemination of personal information.

**Education, Supervision and Monitoring**

It shall be the responsibility of all District employees to be knowledgeable of the Board's policies and administrative guidelines and procedures. Further, it shall be the responsibility of all employees, to the extent prudent to an individual's assignment to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

The Superintendent shall provide for appropriate training for District employees and for students who use the District's computer network and have access to the Internet. Training provided shall be designed to promote the District's commitment to:

* The standards and acceptable use of the District's network and Internet services as set forth in District policy;
* Student safety in regards to use of the Internet, appropriate behavior while using, but not limited to, such things as social networking Web sites, online opportunities and chat rooms; and cyberbullying awareness and response; and compliance with E-rate requirements of the Children's Internet Protection Act.

While training will be subsequently provided to employees under this policy, the requirements of the policy are effective immediately. Employees will be held to strict compliance with the requirements of the policy and the accompanying regulation, regardless of whether training has been given.

The Superintendent is responsible for the implementation of this policy and for establishing and enforcing the District's electronic information services guidelines and procedures for appropriate technology protection measures (filters), monitoring, and use.

*Adopted*: date of Manual adoption

LEGAL REF.: A.R.S. 13-2316

 13-3506.01

 13-3509

 15-341

 34-501

 34-502

 20 U.S.C. 9134, The Children's Internet Protection Act

 47 U.S.C. 254, Communications Act of 1934 (The Children's

 Internet Protection Act)







## Wireless Networking and Access

This policy establishes standards that must be met when wireless communications equipment is connected to Nogales Unified School District networks. The policy prohibits access to district networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the Information Technology Department are approved for connectivity to district networks.

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of TESD’s internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to district networks do not fall under the purview of this policy.

### Approved Equipment

All wireless LAN access must use district approved products and security configurations.

### Monitoring of Uncontrolled Wireless Devices

* All district locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect, classify, and disrupt communication with unapproved wireless access points.
* All district locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect the presence of wireless devices forming a connection between the network and any wireless network. This would include laptops that are serving as a bridge between wired and wireless networks.
* In district locations where wireless LAN access has been deployed, wireless intrusion detection systems will also be deployed to monitor for attacks against the wireless network. The wireless intrusion detection system shall be integrated with the wireless LAN access system whenever possible.

### Authentication of Wireless Clients

* All access to wireless networks must be authenticated.
* The district’s existing password policy must be followed for access to wireless networks.
* The strongest form of wireless authentication permitted by the client device must be used. For the majority of devices and operating systems, WPA or WPA2 with 802.1x/EAPPEAP must be used. WPA2 is preferred wherever possible.
* Where 802.1x authentication is used, mutual authentication must be performed. Client devices must validate that digital certificates presented by the authentication server are trusted and valid. Under no circumstances may clients disable validation of server certificates and globally trust any certificate presented.
* EAP methods that do not support certificate-based mutual authentication may not be used.
* EAP methods that exchange authentication credentials outside of encrypted tunnels may not be used. These methods include EAP-MD5 and LEAP.
* When legacy devices that do not support WPA or WPA2 must be used on a wireless network, they will be isolated from all other wireless devices and will be restricted to the minimum required network access. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network.
* Any user with an account in a district user database shall be able to authenticate at any district location where wireless access is present.

### Encryption

* All wireless communication between district devices and district networks must be encrypted. Wireless networks providing only Internet access for guest users are exempted from this requirement.
* The strongest form of wireless encryption permitted by the client device must be used. For the majority of devices and operating systems, WPA using TKIP encryption or WPA2 using AES-CCM encryption must be used. WPA2 with AES-CCM is preferred wherever possible.
* Client devices that do not support WPA or WPA2 should be secured using VPN technology such as IPSEC where allowed by the client device.
* The use of WEP requires a waiver from the Information Technology Department. Client devices that require the use of WEP must be isolated from all other wireless devices and will be restricted to the minimum required network access. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network.

### Access control policies

* Access to network resources through wireless networks should be restricted based on the business role of the user. Unnecessary protocols should be blocked, as should access to portions of the network with which the user has no need to communicate.
* Access control enforcement shall be based on the user’s authenticated identity, rather than a generic IP address block. This is also known as “identity-based security.”
* The access control system must be implemented in such a way that a malicious inside user is unable to bypass or circumvent access control rules.
* Access control rules must use stateful packet inspection as the underlying technology.

### Client security standards

Where supported by the client operating system, the wireless network will perform checks for minimum client security standards (client integrity checking) before granting access to the district network. Specifically:

* All wireless clients must run approved anti-virus software that has been updated and maintained in accordance with the district’s anti-virus software policy.
* All wireless clients must run host-based firewall software in accordance with the district’s host security policy.
* All wireless clients must have security-related operating system patches applied that have been deemed “critical” in accordance with the district’s security policy.
* All wireless clients must be installed with district-standard wireless driver software.
* Clients not conforming to minimum security standards will be placed into a quarantine condition and automatically remediated.
* Client operating systems that do not support client integrity checking will be given restricted access to the network according to business requirements.

### Wireless guest access

* Wireless guest access will be available at all facilities where wireless access has been deployed.
* All wireless guest access will be authenticated through a web-based authentication system.
* A single username/password combination will be assigned for all guest access. The password for guest access will be changed monthly and distributed to local facility managers.
* Wireless guest access is available from the hours of 7:00 until 20:00 local time.
* Guest access will be restricted to a default filtering policy that is most restrictive.

## Password Requirements and Change Policy

Passwords for domain user accounts and local user accounts must meet a number of requirements for complexity and longevity. These requirements are enforced by Active Directory and Microsoft Group Policies.

* **Enforce Password History** is set to retain the previous 10 passwords. Users must cycle through 10 unique passwords before an old password may be used.
* **Maximum Password Age** is set to 6 months. Users must change their password every 6 months.
* **Minimum Password Age** is set to 1 day. Users must keep new passwords at least 1 day before changing. This prevents quickly cycling through the retained password history.
* **Minimum Password Length** is set to 8 characters
* **Strong Password Requirements** include 7 or more non-repeating characters and a combination of upper and lower case letters, numbers and special characters, e.g. ^,\*,$,~,?.

Passwords for District Voicemail systems must meet the following requirements for complexity and longevity.

* **Maximum Password Age** is set to 2 months. Users must change their password every 2 months.
* Strong Password Requirements include 4 or more characters

## Employee User Account Creation

Domain, Active Directory and Email accounts are created for each employee upon hire. Human resources notify the Information Technology Department of impending hires, start date, location, title and supervisor. Permissions and access to necessary systems is determined from that information and the required accounts are created.

## Employee Termination and Process for removing employees from the network

### Overview

IT Process for Employee Transfers, Terminations and Employee Related Security Threats

### Purpose

The IT department has the responsibility to remove access for employees at the time of termination, transfer or when there is an identified security risk to the District. Standard processes are used when there is a normal transition (separation or transfer) through the District’s Human Resources Department and IT Departments. Emergency processes are utilized when there is a perceived security issue requiring an employee’s immediate access termination or suspension.

### Standard Procedure

The standard procedure is used to remove employee access from the District’s network and systems when employees are processed through the Human Resources (HR) department and no perceived security threat has been identified or communicated to IT. HR will notify IT of personnel changes by periodically sending files of personnel changes to pre-designated IT employees who will remove access to all systems. Directors or their designee may request access to be removed or suspended for employees leaving their departments prior to HR reports being sent to IT through the Visions Personnel Action Request (PAR). IT will work with departments to ensure data is saved or transitioned to other users where appropriate.

###  Enforcement

Since this process is critical to the security of the organization and its users, this policy must be enforced by District administrators through annual review and auditing.

## Physical Security

This policy addresses best practice requirements to protect physical data security.

Facilities containing district networking, data storage and transmission equipment must follow the following controls to prevent unauthorized physical access. These facilities are defined as the data center, MDF, IDF, demarcation and riser closets. These controls also pertain to equipment cabinets installed in various classrooms, as appropriate.

* Access to facilities will be based on role or function with minimum access necessary to perform the individual’s job function.
* Regular review (minimum interval of 6 months) of authorization for facility access of staff and vendors to ensure that facility access is limited to only those with a business need for physical access to the facility.
* Logging of vendor access. All physical access to facilities by vendors must be logged for entry time, exit time, purpose, and staff member who allowed facility entry. Vendors should always be escorted by workforce members.
* All such facilities must be secured from unauthorized access. Appropriate physical controls include door keys, where distribution is restricted, controlled and reviewed at least once per year.
* Environmental controls should be in place for any facility covered under this policy. Reasonable attempts must be made to implement protections against power outages, fire, water damage, temperature extremes and other environmental hazards.
* Creation of inventory of hardware and electronic media residing in each facility.
* Maintain maintenance records, documentation of repairs and modifications to physical components, and records documenting the movement of hardware or electronic media in or out of each facility.

# IT Contingency Plan

This document contains the Contingency Plan for the IT System. It is intended to serve as the centralized repository for the information, tasks, and procedures that would be necessary to facilitate the IT System management’s decision-making process and its timely response to any disruptive or extended interruption of the department's normal business operations and services. This is especially important if the cause of the interruption is such that a prompt resumption of operations cannot be accomplished by employing only normal daily operating procedures.

In terms of personnel and financial resources, the information tasks and procedures detailed in this plan represent the IT System management’s demonstrated commitment to response, resumption, recovery, and restoration planning. Therefore, it is essential that the information and action plans in this plan remain viable and be maintained in a state of currency in order to ensure the accuracy of its contents. To that end, this introduction is intended to introduce and familiarize its readers with the organization of the plan.

It is incumbent upon every individual who is in receipt of the IT System Contingency Plan, or any parts thereof, or who has a role and/or responsibility for any information or materials contained in the document, to ensure that adequate and sufficient attention and resources are committed to the maintenance and security of the document and its contents.

Since the information contained in this document describes IT System management’s planning assumptions and objectives, the plan should be considered a sensitive document. All of the information and material contents of this document should be labeled, “Limited Official use”.

The IT System’s management has recognized the potential financial and operational losses associated with service interruptions and the importance of maintaining viable emergency response, resumption, recovery and restoration strategies.

The IT System Contingency Plan is intended to provide a framework for constructing plans to ensure the safety of employees and the resumption of time-sensitive operations and services in the event of an emergency (fire, power or communications blackout, tornado, hurricane, flood, earthquake, civil disturbance, etc.)

Although the IT System’s Contingency Plan provides guidance and documentation upon which to base emergency response, resumption, and recovery planning efforts, it is not intended as a substitute for informed decision-making. Business process managers and accountable executives must identify services for which disruption will result in significant financial and/or operational losses. Plans should include detailed responsibilities and specific tasks for emergency response activities and business resumption operations based up-on pre-defined time frames.

Constructing a plan and presenting it to senior management may satisfy the immediate need of having a documented plan. However, this is not enough if the goal is to have a viable response, resumption, recovery, and restoration capability. In order to establish that capability, plans, and the activities associated with their maintenance (i.e. training, revision, and exercising) must become an integral part of IT System’s operations.

A Contingency Plan is not a one-time commitment and is not a project with an established start and end date. Instead, a Contingency Plan is an on-going, funded business activity budgeted to provide resources required to:

* Perform activities required to construct plans
* Train and retrain employees
* Develop and revise policies and standards as the department changes
* Exercise strategies, procedures, team and resources requirements
* Re-exercise unattained exercise objectives
* Report on-going continuity planning to senior management
* Research processes and technologies to improve resumption and recovery efficiency
* Perform plan maintenance activities

Developing a Contingency Plan that encompasses activities required to maintain a viable continuity capability ensures that a consistent planning methodology is applied to all of the IT System Contingency Plan elements necessary to create a viable, repeatable and verifiable continuity capability include:

* Implementing accurate and continuous vital records, data backup, and off-site storage
* Implementing capabilities for rapid switching of voice and data communication circuits to alternate site(s)
* Providing alternate sites for business operations
* Constructing a contingency organization
* Implementing contingency strategies

## PURPOSE

The purpose of this plan is to enable the sustained execution of mission critical processes and information technology systems for IT System in the event of an extraordinary event that causes these systems to fail minimum production requirements. The IT System Contingency Plan will assess the needs and requirements so that IT System may be prepared to respond to the event in order to efficiently regain operation of the systems that are made inoperable from the event.

## SCOPE

Insert information on the specific systems, locations, Facility divisions, technical boundaries and physical boundaries of the IT System Contingency Plan.

## PLAN INFORMATION

The Contingency Plan contains information in two parts related to the frequency of updates required. The first part contains the plan’s static information (i.e. the information that will remain constant and will not be subject to frequent revisions). The second part contains the plan’s dynamic information (i.e. the information that must be maintained regularly to ensure that the plan remains viable and in a constant state of readiness). This dynamic information is viewed as the action plan. The action plan should be considered a living document and will always require continuing review and modification in order to keep up with the changing IT System environment.

The static information part of the Contingency Plan is contained in a MS-Word file and printed as part of this document. This static information should be read and understood by all employees, users, and administrators of the IT System, or at least by those individuals who are involved in any phase of business response, resumption, recovery, or restoration.

The dynamic information resides in the database of the “**backup2 Server**” and will be printed as output for the appendixes of this document. By using the database, dynamic in-formation that is vital to the survival of the IT System will be easy to manage and update. The web-enabled database is designed for maintenance of personnel contact lists, emergency procedures, and technical components. It is already in operation for some in-house agencies.

For ease of use and reference, the static and dynamic information is maintained separately. While it is necessary to be familiar with the static information during resumption, it should not be necessary to read that information at the time of the event. The completed action plan of dynamic information provides all of the necessary lists, tasks, and reports used for response, resumption, or recovery.

# CONTINGENCY PLAN OVERVIEW

## OBJECTIVES

The IT System is dependent on the variety of systems classified as General Support Systems (GSSs), which provide mission critical functions of connectivity, Internet access, and email, or Major Applications (MAs) which are specific software programs written to IT System.

The primary focus of a contingency plan revolves around the protection of the two most important assets of any organization: personnel and data. All facets of a contingency plan should address the protection and safety of personnel and the protection and recovery of data. The primary objective of this plan is to establish policies and procedures to be used for information systems in the event of a contingency to protect and ensure functioning of those assets. This includes establishing an operational capability to process pre-designated critical applications, recovering data from off-site backup data sets, and restoring the affected systems to normal operational status. The plan seeks to accomplish the following additional objectives:

* Minimize the number of decisions which must be made during a contingency
* Identify the resources needed to execute the actions defined by this plan
* Identify actions to be undertaken by pre-designated teams
* Identify critical data in conjunction with customers that will be recovered during the Hot Site phase of recovery operations
* Define the process for testing and maintaining this plan and training for contingency teams

## ORGANIZATION

In the event of a disaster or other circumstances which bring about the need for contingency operations, the normal organization of the Technology Department will shift into that of the contingency organization. The focus of the IT System will shift from the current structure and function of “business as usual” to the structure and function of an IT System working towards the resumption of time-sensitive business operations. In this plan, the IT System’s contingency organization will operate through phases of response, resumption, recovery, and restoration. Each phase involves exercising procedures of the IT System’s Contingency Plan and the teams executing those plans. The teams associated with the plan represent functions of a department or support functions developed to respond, resume, recover, or restore operations or facilities of the IT System and its affected systems. Each of the teams is comprised of individuals with specific responsibilities or tasks, which must be completed to fully execute the plan. Primary and alternate team leaders, who are responsible to the plan owner, lead each team.

Each team becomes a sub-unit of the IT System’s contingency organization. Coordination teams may be singular for the IT System, whereas technical teams will likely be system specific. Figure 3-1, Contingency Planning Organizational Chart, shows the base organizational structure. The teams are structured to provide dedicated, focused support in the areas of their particular experience and expertise for specific response, resumption and recovery tasks, responsibilities, and objectives. A high degree of interaction among all teams will be required to execute the plan. Each team’s eventual goal is the resumption/recovery and the return to stable and normal business operations and technology environments. Status and progress updates will be reported by each team leader to the plan owner. Close coordination must be maintained with IT System and N.U.S.D management and each of the teams throughout the resumption and recovery operations.

The IT System contingency organization’s primary duties are:

* To protect employees and information assets until normal business operations are resumed.
* To ensure that a viable capability exists to respond to an incident.
* To manage all response, resumption, recovery, and restoration activities.
* To support and communicate with employees, system administrators, security officers, and managers.
* To accomplish rapid and efficient resumption of time-sensitive business operations, technology, and functional support areas.
* To ensure regulatory requirements are satisfied.
* To exercise resumption and recovery expenditure decisions.
* To streamline the reporting of resumption and recovery progress between the teams and management of each system.

Figure 3-1 Contingency Planning Organizational Chart

## CONTINGENCY PHASES

The IT Systems Contingency Plan Coordinator, in conjunction with Facility Network management will determine which Teams/Team members are responsible for each function during each phase. As tasking is assigned, additional responsibilities, teams, and task lists need to be created to address specific functions during a specific phase.

### NOTIFICATION/ACTIVATION PHASE

The Notification/Activation Phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel (including when key Department personnel are unreachable), assess system damage, and implement the plan. At the completion of the Notification/Activation Phase, Department staff will be prepared to perform contingency measures to restore system functions on a temporary basis, as defined in the plan.

Events requiring activation of the IT Contingency Plan may occur with or without prior notification. In either situation, notification procedures in the IT Contingency Plan must be detailed and include methods (e-mail, phone, and mass media) to contact people during both business and non-business hours.

The DAMAGE ASSESSMENT TEAM is to perform the damage assessment as soon as possible after the event has occurred. Damage Assessment Team members must be the first staff notified and must include staff in the closest physical proximity to the main processing site where the event would have occurred.

The CONTINGENCY PLAN COORDINATOR will analyze the results of the damage assessment and determine whether the criteria for plan activation are met. The criteria will be defined and documented based on system-specific requirements and may include:

* Safety of personnel
* Extent of damage to the facility
* Extent of damage to the system
* Criticality of the system (mission critical, important, or supportive)
* Anticipated duration of the disruption.

If the criteria have been met, the CONTINGENCY PLAN COORDINATOR will activate the plan to the extent necessary. Different events may require the plan to be activated to different levels, or only portions of the plan to be activated. For example, a loss of data might require the recovery of backup tapes, but the destruction of the area surrounding the facility might require a move to the alternate location. The recovery teams needed to execute the plan after activation must be notified accordingly.

### RECOVERY PHASE

Recovery phase activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or alternate facility. At the completion of the Recovery Phase, the IT system will be operational and performing the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site.

### RECONSTITUTION PHASE

In the Reconstitution Phase, recovery activities are terminated and normal operations are transferred back to the original facility. Until the primary system is restored and tested, the contingency system will continue to be operated. Teams will be designated to specifically assist in reconstitution activities that may be occurring at the same time as recovery procedures at an alternate site. The potential for recovery and reconstitution activities to overlap should be considered when planning the number of teams and personnel required.

The following are some of the major activities that may occur during the reconstitution phase:

* Ensuring adequate infrastructure support (electric, water, and telecommunications)
* Installing system hardware, software, and firmware
* Establishing connectivity and interfaces with network components and external systems
* Testing system operations to ensure full functionality
* Backing up operational data on the contingency system and uploading to restored system
* Terminating contingency operations
* Shutting down contingency system
* Removing and/or relocating all sensitive materials at the contingency site
* Arranging for recovery personnel to return to the original facility

## ASSUMPTIONS

* Telecommunications connectivity, Electrical Power, Third-Party Data Services will be available for full restoration.
* All existing hardware is undamaged and operational.
* Parts are on-hand if needed.
* All departments are fully staffed.
* Transportation is available if needed.
* That all necessary Memorandums of Agreement (MOAs) and Memorandums of Under-standing (MOUs) have been executed.

## CRITICAL SUCCESS FACTORS AND ISSUES

* Absolute commitment by senior management to Contingency Planning and Disaster Recovery.
* Budgetary commitment to Disaster Recovery.
* Modifications and improvements to the current scheduling procedures for the retention and transportation of back up files to the offsite storage facility.
* Development and execution of the necessary Memorandums of Agreement (MOAs), Memorandums of Understanding (MOUs), and Service Level Agreements (SLAs).

## MISSION CRITICAL SYSTEMS/APPLICATIONS/SERVICES

IT Systems has identified the applications and services shown in Figure 3.2 as mission critical. These systems/applications/services must be recovered at the time of disaster in the following order due to critical interdependencies:

| SYSTEMS ACRONYM | SYSTEM NAME |
| --- | --- |
| MS-AD-DC |  |
| Internet Connectivity |  |
| Visions |  |
| PowerSchool SIS |  |
| Kronos |  |
| VoIP |  |
| Internet Content Filter |  |
| Network Firewall |  |

Figure 3-2 Mission Critical Systems

## THREATS

This contingency plan seeks to consider the entire range of probable and possible threats that present a risk to the organization. From this range of threats, likely scenarios can be developed and appropriate strategies applied. This disaster recovery plan has been designed to be flexible enough to respond to extended business interruptions, as well as major disasters.

### PROBABLE THREATS

The table depicts the threats most likely to impact the N.U.S.D Data Centers and components of IT Systems and their management. The specific threats that are represented by (XX) are considered the most likely to occur within the IT Systems environment.

| Probability of Occurrence | High | Medium | Low |
| --- | --- | --- | --- |
| **Air Conditioning Failure** | X |  |  |
| **Aircraft Accident** |  |  | X |
| **Blackmail** |  | X |  |
| **Bomb Threats** |  | X |  |
| **Chemical Spills / HazMat** |  |  | X |
| **Cold / Frost / Snow** |  |  | X |
| **Communications Loss** | XX |  |  |
| **Data Destruction/Breach** |  | X |  |
| **Denial of Service (DDoS)** |  | X |  |
| **Earthquakes** |  |  | X |
| **Fire** |  |  | X |
| **Flooding / Water Damage** |  |  | X |
| **Nuclear Mishaps** |  |  | X |
| **Power Loss / Outage** | XX |  |  |
| **Sabotage / Terrorism** |  |  | X |
| **Storms / Hurricanes** |  | X |  |
| **Vandalism / Rioting** |  | X |  |
| **Virus/Malware/Ransomware** | XX |  |  |

Figure 3-3 Probability of Threats

# SYSTEM DESCRIPTION

In this section include information for each system under ownership or controlling authority of the IT System. Controlling authority assumes that a function or mission element of a Facility/System has been contracted to an outside entity that provides the facilities, hardware, and software and personnel required to perform that task IT System Facility retain the oversight of that operation and therefore are the controlling activity for that system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| System/Service | Description | Vendor | RPORecovery Point | RTORecovery Time |
| MS-AD-DC |  |  | 8 hr. | 4 hr. |
| Internet Connectivity |  |  | N/A | 4 hr. |
| Visions |  |  | 8 hr. | 5 days |
| PowerSchool |  |  | 8 hr. | 3 days |
| Kronos |   |  | 8 hr. | 5 days |
| VoIP |  |  | N/A | 4 hr. |
| Internet Content Filter |  |  | N/A | 4 hr. |
| Network Firewall |  |  | N/A | 4 hr. |
|  |  |  |  |  |

## PHYSICAL ENVIRONMENT

The table below indicates the physical location or connection point for each critical IT System.

|  |  |  |
| --- | --- | --- |
| System/Service | Description | Location |
| MS-AD-DC |  |  |
| Internet Connectivity |  |  |
| Visions |  |  |
| PowerSchool |  |  |
| Kronos |  |  |
| VoIP |  |  |
| Internet Content Filter |  |  |
| Network Firewall |  |  |
|  |  |  |

## TECHNICAL ENVIRONMENT

The Nogales Unified School District consists of a diverse infrastructure of networking systems designed to connect each school to the District Data Center at 451 N. Arroyo Blvd. The District Data Center facilitates connectivity to the various applications and data repositories as well as access to the Internet and telecommunications.

Detailed hardware inventories, network configurations, licensing and vendor contact information is maintained on the **XXXXX** Server.

### Internet

The District accesses the Internet via Fiber Optic connection provided by XXXX Broadband Services at 10 Gbps.

### Wide Area Network

Each school in the District is connected to the District Data Center via dedicated Point to Point (PTP) Fiber Optic circuits leased from XXXXXX Broadband Services at 10 Gbps.

### Voice over IP (VoIP)

Telephone communications is provided via ShoreTel Voice Switches at each school and the District Office.

### Wireless Local Area Network (WLAN)

Each school and building in the District has an installation of Meraki Wireless Access Points to facilitate wireless access to the District’s network, applications, data resources and Internet connectivity. Each Access Point (AP) is physically connected to a Cisco Data Switch via 1 Gbps Copper Category 5e or Category 6 Ethernet cabling. The system will be a Meraki cloud based Wireless Controller.

### UPS and Backup Power

Each networking closet (IDF and MDF) at each school is equipped with backup power devices sufficient to maintain power during a brief outage of 15-20 minutes. The District Data Center has battery backup power sufficient to maintain system operation during an outage of 2-6 hours. During extended outages systems may be deactivated systematically to prevent hardware damage or software corruption.

### Alternate Data Center

The District will use the Nogales High School Data Center at 1905 Apache Blvd. as an alternate site in the event of an outage at the Main Data Center. The NHS Data Center can be considered a “Warm” Site in that it functions normally according to the High School needs and operations. This site remains operational during the year but will require additional equipment and preparation before transitioning to the alternate Data Center during an emergency situation.

The ADMINISTRATIVE MANAGEMENT TEAM will perform a semi-annual assessment of the Alternate Site as compared to the District Data Center to determine which equipment must be replaced or added in the event of Contingency Plan Activation. A secondary list of equipment to be purchased after Plan Activation will also be maintained. Due to budgetary considerations, this equipment will not be kept on hand but purchased if needed to bring the Alternate Site online.

The Hardware Inventory section in this document will list equipment at each location, including equipment that must be procured prior to restoration of services at the Alternate Site.

# PLAN

## PLAN MANAGEMENT

### CONTINGENCY PLANNING WORKGROUPS

The development of recovery strategies and work-arounds require technical input, creativity, and pragmatism. The best way to create workable strategies and cohesive teams that leverage out-of-the-box thinking is to involve management and information resource management personnel in an ongoing informative dialogue. NUSD management has developed and is facilitating Contingency Planning workgroups to assist in the development and review of strategies, teams, and tasks. Refer to Figure 3-1 above for leadership assignments for each workgroup.

### CONTINGENCY PLAN COORDINATOR

The Assistant District Superintendent will serve the roll of Contingency Plan Coordinator with the Technology Director acting as alternate.

This person will coordinate strategy development with Contingency Planning Workgroups, System Contingency Coordinator, Team Leaders, Business Process Owners, and Management. The Contingency Planning Coordinator will work closely with system technical managers to ensure the viability of the IT Systems Contingency Plan. The Contingency Plan Coordinator will manage contingency teams that are not system specific (see section 5.2).

### SYSTEM CONTINGENCY COORDINATORS

A coordinator and an alternate has been appointed for EACH SYSTEM under ownership or controlling authority of the IT System by Superintendent and system owners. Their primary task will be to monitor and coordinate the NUSD contingency planning, training and awareness, exercises, and testing. Additionally, each person will manage contingency teams (see Section 5.2) that are assigned specifically to their system and report directly to the Contingency Plan Coordinator.

### INCIDENT NOTIFICATION

The facilities managers for the locations where the critical components of the IT Systems are located have been provided with the telephone numbers of NUSD Emergency Response Team members (see Section 5.2). Upon notification, the team will meet in ***District Office Conference Room*** for the purpose of conducting initial incident assessment and issuing advisory reports of status to the IT System and NUSD management. If the facilities manager, emergency response personnel, or NUSD Emergency Response Team Leader has determined that the building cannot be entered, the alternate meeting place will be the ***Maintenance Conference Room.***

### INTERNAL PERSONNEL NOTIFICATION

A Contact Database consisting of home addresses, telephone numbers and emergency contact information for each member of the Crisis Management Team and Disaster Recovery Teams has been created and resides in a database on the **XXXX** server. This personnel database will be maintained and updated continuously and made available to each stakeholder of the Contingency Plan.

### EXTERNAL CONTACT NOTIFICATION

A list of contacts for each service provider, vendor or supplier of critical systems covered in this contingency plan has been created and resides in a database on the **XXXX** server. This database will be maintained and updated continuously and made available to each stakeholder of the Contingency Plan.

### MEDIA RELEASES

All incident related information (printed or spoken), concerning the NUSD will be coordinated and issued through the Superintendent’s Office.

## TEAMS

The following are teams that will be assigned to execute the contingency plan. Depending on the type of outage experienced certain teams may not be required to act.

### DAMAGE ASSESSMENT TEAM

The Damage Assessment Team is a technical group responsible for assessing damage to the Facility/System and its components. It is composed of personnel with a thorough understanding of hardware and equipment and the authority to make decisions regarding the procurement and disposition of hardware and other assets. This team is primarily responsible for initial damage assessment, accounting of damage assessment, loss minimization, salvage and procurement of necessary replacement equipment and interfaces. This team may include vendor representatives.

The Damage Assessment Team will enter the facility as soon as they have received permission to do so from emergency services. A written detailed account should be made of the general status of the work area, with specific attention to the condition of hardware, software, furnishings, and fixtures. Recommendations should be made that all damaged equipment, media, and documentation be routed immediately to disaster recovery and restoration experts for a determination as to its ability to be salvaged or restored.

|  |  |  |
| --- | --- | --- |
| Name / Position | Position | Contact Number |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### ADMINISTRATIVE MANAGEMENT TEAM

The Administrative Management Team coordinates Primary and Alternate Site security and specialized clerical and administrative support for the Contingency Plan Coordinator and all other teams during disaster contingency proceedings. The Administrative Team may also assist groups outside the information resources area as needed. The Administrative Team is responsible for reassembling all documentation for standards, procedures, applications, programs, systems, and forms, as required at the backup site. The Administrative Team is responsible for arranging for transportation of staff, equipment, supplies, and other necessary items between sites.

| Team Contact | Position | Contact Number |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### IT SYSTEMS TEAM

IT Systems consists of multiple sub-teams responsible for the assessment and restoration of critical IT Systems.

####  OPERATIONS

The Operations Team consists of operators responsible for running emergency production for critical systems, coordinating with Off-Site Storage Team to ensure that applications system data and operating instructions are correct, and with the Communications Team to advise of the production status and any unusual problems requiring assistance.

| Team Contact Name | Position | Contact Number |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

#### COMMUNICATIONS

The Communications Team is composed of IT Systems communications specialists responsible for restoring voice, data, and video communications links between users and the computers, regardless of location in the event of a loss or outage. This Team will work closely with the current Communication vendor (Conterra Broadband) to implement the recovery plan.

| Team Contact | Position | Contact Number |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

#### CONFIGURATION MANAGEMENT TEAM

The Configuration Management Team is composed of individuals with teleprocessing skills. They work closely with the Communications Teams in establishing voice and data communication capabilities.

|  |  |  |
| --- | --- | --- |
| Team Contact | Position | Contact Number |
|  |  |  |
|  |  |  |
|  |  |  |

#### OFF-SITE STORAGE

The Off-site Storage Team is responsible for retrieving backup copies of operating systems applications, systems, applications data, and ensuring security of the data, backup facilities, and original facilities. The team is composed of members of Technology Dept. familiar with vital records archival and retrieval.

|  |  |  |
| --- | --- | --- |
| Team Contact | Position | Contact Number |
|  |  |  |
|  |  |  |

#### USER ASSISTANCE

The User Assistance team is composed of individuals with application use knowledge. The team is made up of major user area managers, production control, and applications lead analysts responsible for coordination and liaison, with the information resources staff for applications recovery and restoration of data files and databases.

| Team Contact | Position | Contact Number |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### FACILITIES TEAM

The Facilities Team is responsible for arranging for the primary and backup facilities and all components.

| Team Contact | Position | Contact Number |
| --- | --- | --- |
|  |  |  |
|  |  |  |

### PROCUREMENT TEAM

The Procurement Team consists of persons knowledgeable of the information resources and supplies inventory and the budgetary, funding, and acquisition processes responsible for expediting acquisition of necessary resources.

| Team Contact | Position | Contact Number |
| --- | --- | --- |
|  |  |  |
|  |  |  |

## DATA COMMUNICATIONS

The level of data connectivity required will be determined by the severity and anticipated length of the outage. Data communications specifications are documented in APPENDIX H, Communication Requirements, in this plan. These requirements will be the basis for systems restoration at the designated replacement facility.

## BACKUPS

* File data and essential systems are backed up twice daily on site at the district data center using Datto a cloud based solution.
* Full backup of all servers, i.e. file, Hyper V, Domain Controllers, SQL, Time Keeping Server, Visions, is performed twice daily.
* A secondary backup is accessed via cloud. This backup is scheduled by application or server to take advantage of decreased utilization on network resources.
* A backup job is considered successful if completed with zero critical errors.
* Failed backup jobs may be re-run until completed with zero critical errors.
* Successful backups are retained for 1 month.
* Backups are tested quarterly to confirm data can be restored. This is a test of Backup System Integrity, as opposed to a disaster recovery test.

## Restoration Policy

* Requests for recovery of data files or email but be submitted through the work order process
* All recovery efforts will be consistent with established data retention policies.
* On site backed up data will be restored to users within 1 working day of request.
* Data backups may not be used as a means of archiving data or maintaining a versioned history of data.
* Individual workstations are not included in backup procedures.

## VITAL RECORDS/DOCUMENTATION

Vital records are any documents or documentation that is essential to the operations of an organization, such as personnel records, software documentation, legal documentation, legislative documentation, benefits documentation, etc.

Vital records and important documentation are scanned to electronic format and stored on District data servers. These files are secured according to individual access needs and security policies. The files are also included in the file backup as outlined in section 5.4.

Copies of the following documentation are also kept in electronic format and maintained off site:

* Security related Information Technology (IT) policy & procedure memorandum, circulars, publications
* Letters of delegation for key Information System security personnel
* Complete hardware and software listings
* Internal security, Information System audits
* Detailed IT architecture schematics (logical/physical, network, devices)
* System testing plans/procedures
* Review and approval of plans/procedures
* System Configuration
* Review and approval of proposed configuration
* Changes made to the system configuration
* Evaluation of changes for security implications
* Technical standards for system design, testing and maintenance to reflect security objectives
* Contingency plans for incident response procedures and backup operations
* Data backup/restoration procedures
* Reports of security related incidents
* Sensitivity and criticality determination
* Baseline security checklist for each system
* Software licensing information

## OFFICE EQUIPMENT, FURNITURE AND SUPPLIES

An inventory of workplace supplies (pens, pencils, paper, etc.) and available office furniture shall be kept updated and current. Facilities management and the Business Office representatives will review the inventory to identify items that can be relocated quickly to a replacement facility in the event of a disaster.

An inventory of survival supplies will be maintained, including bottled drinking water, personal products, and food rations, in the event personnel cannot be evacuated or are temporarily prevented from leaving the confines of the building due to weather conditions.

## RECOMMENDED TESTING PROCEDURES

This Contingency Plan will be maintained routinely and tested annually. The scope, objective, and measurement criteria of each exercise will be determined and coordinated by the Contingency Plan Coordinator on a “per event” basis. The purpose of exercising and testing the plan is to continually refine resumption and recovery procedures to reduce the potential for failure.

Testing will be conducted outside of normal school hours and will be planned so as not to interfere with instruction or teacher schedules.

The Contingency Plan Coordinator, System Coordinators, and Team Leaders, together with system owners will determine end-user participation.

Each test shall address the following areas:

* System recovery on alternate hardware from backup media
* Coordination among functional Teams
* Internal and External Connectivity
* System performance on alternate equipment
* Return to normal operations
* Notifications procedures

In addition to annual Functional testing of the plan, semi-annual reviews and walkthroughs of various elements of the plan will be conducted by IT SYSTEMS TEAM to maintain familiarity with the required technologies and make adjustments as necessary. These tests can be performed with no actual recovery operations occurring.

Test results and lessons learned shall be documented in the CONTINGENCY LOG included in this document.

All tests should meet the following objectives:

* Verify that all individuals and team leaders understand their role
* Resolve all questions and ambiguities during the test
* Provide Administrative Teams with a summary outlining successes and areas for improvement
* Initiate improvements to the plan based on discussions, observations and findings identified during the tests.

The scope of Contingency Plan testing may include recovery of all systems necessary as well as communications and network components and interfaces. Recovery time objectives for all components will be tested and recorded.

# Logging and monitoring audit policy

**Introduction**

Audit Monitoring is a method used by NUSD to confirm that the security practices and controls in place are being adhered to and are effective. Audit Monitoring consists of activities such as the review of:

* Firewall logs
* User account logs
* Network scanning logs
* Active Directory security logs

**Definitions**

Information System

Being connected to a NUSD Information System includes:

* If you have a network capable device (ex. laptop)
* If you have a wireless capable device (ex. laptop, smartphone, tablet)

**Purpose**

The purpose of this policy is to ensure that Audit monitoring controls are in place, are effective, and are not being bypassed. One of the benefits of Audit monitoring is the early identification of wrongdoing, new security vulnerabilities, or new unforeseen threats to our information resources. Early identification can help block the threat or vulnerability to NUSD’s core Information Systems.

**Policy**

NUSD shall utilize auditing tools to perform electronic scans of their core Information Systems. The IT Department will review the audit monitoring logs periodically or when the need arises. Any anomalies will be addressed accordingly.

These scans may include:

* User and/or system level access to any computer
* Access to information that may be produced, transmitted or stored on any of NUSD’s Servers or Computers
* Password Auditing
* Penetration Testing

In addition, the following files of these systems will be checked for signs of exploitation:

* Firewall logs
* User account logs
* Network scanning logs
* System error logs
* Application logs
* Data backup logs

# Controlling administrative access/rights

**Introduction**

Controlling Administrator rights is made possible by leveraging the Active Directory Services ability to provide, revoke, or modify user authentication across our organization.

 **Purpose**

The purpose of this Guideline is to instruct individuals providing IT support on the appropriate use of Administrator Access to NUSD Active Directory Services and Network resources.

**Definitions**

Administrator Access is defined as a level of access above that of a normal user.  This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms.  In a traditional Microsoft Windows environment, members of the Power Users, Domain Administrators, and Enterprise Administrators groups would all be considered to have Administrator Access.

*Delegation of administration* refers to establishing access control lists on organizational units and accounts in Active Directory.

*Active Directory* is a Windows OS directory service that facilitates working with interconnected network resources in a unified manner.

**Policy**

The Information Technology Department will grant Domain Administrator and Delegation of Administration rights, as appropriate, to those personnel who require such rights to perform their duties. NUSD will strictly adhere to the principle of least privilege when granting rights. Rights will only be granted under the condition that they are essential for the performance of the grantee’s job.

NUSD’s Information Technology Department will manage and track all users with Domain Administrator and Delegation of Administration rights. Regular review of all access rights will take place at least once bi-annually.

**Guidelines for use of Administrator Access**

Administrator Access to any of NUSD computing resources should only be used for official business use. Use of Administrator Access should be consistent with an individual’s role or job responsibilities as prescribed by management.  When an individual’s role or job responsibilities change, Administrator Access should be appropriately updated or removed.

The following constitutes inappropriate use of Administrator Access to NUSD computing resources.

* Accessing Non-public Information that is outside the scope of specific job responsibilities.
* Exposing or otherwise disclosing Non-public Information to unauthorized persons or entities.
* Using access to satisfy personal curiosity about an individual, system, practice, or other type of entity.

**Failure to adhere to these policies is subject to Acceptable Use Policy penalties.**

# APPENDICES

All items in these appendices are available digitally and accessible from outside the district network. These items are updated frequently as necessary.

1. CONTINGENCY PLAN CONTACT INFORMATION

This appendix includes all points of contact described in the Contingency Plan and key organizational personnel

|  |  |
| --- | --- |
| Emergency Contact | Phone Number |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Contact | Position | Cell |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

| Principal Name | School | Cell |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |

|  |  |  |
| --- | --- | --- |
| Team Contact | Position | Cell |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. EMERGENCY PROCEDURES

For the purposes of this Contingency Plan the procedures outlined below pertain to a complete outage or inaccessibility of the NUSD Data Center at 451 N. Arroyo Blvd., regardless of the type of emergency situation. All other outages to local resources, individual buildings or specific systems will be handled through day to day support and restoration processes required for that situation. For example, an Internet outage affects all users District-Wide but does not, in itself, warrant the enactment of these Emergency Procedures.

* 1. Notification/Activation Phase

In the event of an outage at the NUSD Data Center, members of the IT COMMUNICATIONS TEAM will receive automatic notifications from internal systems indicating potential issues or suspension of service. An initial assessment of the situation is done by members of the Communications team to determine the extent and length of the outage.

All members of the DAMAGE ASSESSMENT TEAM are then notified and assembled as outlined in Section 5.1.4. The following areas are some examples of what could be addressed by the DAMAGE ASSESSMENT TEAM:

* Cause of the emergency or disruption
* Potential and additional disruptions or damage
* Area affected by the emergency
* Status of the physical infrastructure (structural integrity, telecommunications, power, ventilation, heating, air-conditioning)
* Inventory and functional status of IT equipment
* Type of damage to IT equipment and data
* Items to be replaced
* Estimated time to restoration of normal services.

If the outage is determined to be less than 4 hours in length AND the Data Center is still accessible and functioning, there should be no need to continue with the Contingency Plan. With an outage in excess of 4 hours AND/OR loss of the District Data Center proceed to the next phase.

* 1. Recovery Phase

NUSD has setup an alternate site at Nogales High School from which all systems and services can be restored as needed.

DAMAGE ASSESSMENT TEAM

1. Update the Superintendent in order to facilitate public notifications as necessary.
2. Determine what, if any, equipment and resources to be transferred to the alternate site.
3. Begin procurement process of any equipment, supplies or transportation necessary to bring the alternate site online.
4. Continue to monitor and assess situation at main District Data Center for opportunity to restore operations.

ADMINISTRATIVE TEAM

1. Direct and inform each team regarding needs at affected sites.
2. Provide financial and administrative support to transition operations from damaged Data Center to alternate site.
3. Coordinate with stakeholders of each functional area to commence testing of restored data and systems.
4. Coordinate with IT SYSTEMS – USER ASSISTANCE team to support stakeholders during verification of restored systems.
5. Update Superintendent’s office at regular intervals

IT SYSTEMS – COMMUNICATIONS TEAM

1. Contact vendor for emergency Internet service connectivity to alternate site. Coordinate with FACILITIES AND PROCUREMENT TEAMS for necessary resources and access. Goal should be minimum bandwidth necessary to support connectivity to critical systems during outage.
2. Contact current Wide Area Network provider to begin transition of “Hub” from District Data Center to Alternate Site. Point to Point connectivity of each school site will be re-routed to alternate site.
3. Coordinate with IT SYSTEMS – USER ASSISTANCE TEAM as necessary at each school site.

IT SYSTEMS – OFF-SITE STORAGE TEAM

1. Retrieve latest backup media for each system to be restored at alternate site.
2. Identify and assess hardware at alternate site to host critical systems
3. Coordinate with FACILITIES AND PROCUREMENT TEAMS for necessary resources and access.
4. Begin restoration from backup of critical systems at alternate site in anticipation of restoration of connectivity district-wide.
5. Communicate status to ADMINISTRATIVE TEAM.

IT SYSTEMS – CONFIGURATION MANAGEMENT TEAM

1. Gather hardware inventories and network configurations necessary for the restoration and re-routing of connectivity at the alternate site.
	1. Reconstitution phase

DAMAGE ASSESSMENT TEAM

1. Upon determination that main District Data Center is safe and able to resume operation, notify the ADMINISTRATIVE TEAM and prepare to transition from the alternate site.

IT SYSTEMS – COMMUNICATIONS TEAM

1. Coordinate with service providers to verify resumption of Internet and WAN connectivity.
2. Test and verify connectivity and communications at District Data Center.

IT SYSTEMS – OFF-SITE STORAGE TEAM

1. Begin backup of critical systems at alternate site for restoration at District Data Center.
2. Upon completion of backup activities, transfer media to District Data Center for restoration of data and systems.
3. Communicate status to ADMINISTRATIVE TEAM

ADMINISTRATIVE TEAM

1. Direct and inform each team regarding needs at affected sites.
2. Coordinate with stakeholders of each functional area to commence testing of restored data and systems.
3. Coordinate with IT SYSTEMS – USER ASSISTANCE team to support stakeholders during verification of restored systems.
4. Update Superintendent’s office at regular intervals
5. Upon restoration of all systems, reconvene to record lessons learned and determine modifications and corrections to the existing plan.
6. SOFTWARE INVENTORY

This appendix should be populated with the most current data that directly reflects the current software, being tested and evaluated, operational in the acceptance environment pending final review, implemented in production, owned whether onsite or offsite, and deployed by the district. This should include the licensing agreements. A copy of this data should be stored at the offsite storage facility along with the Contingency Plan.

|  |  |
| --- | --- |
| **System** | **Software Version** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. HARDWARE INVENTORY

This appendix should be populated with the most accurate data reflective of the hardware assets currently owned and deployed by the district. In addition, the inventory of the alternate site hardware assets should be included as well. The purchase and implementation of an automated tool could assist in this effort.

* 1. District Data Center

| Rack | Equipment |
| --- | --- |
| Rack 1 | HP Proliant DL380G7 Server - 8 HDD\* |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Rack 2 | Dell PowerEdge R420 Servers - 12 HDD total |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Rack 3 | Dell PowerEdge R710 - 20 HDD total |
|  |  |
|  |  |
|  |  |
| Rack 4 | Dell PowerEdge 2950 - 27 HDD total |
|  |  |
|  |  |
|  |  |
|  |  |
| Rack 5 | Cisco Catalyst 3750X 48 port POE |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Rack 6 | Symmetra LX 16000 Main Cabinet - 5 Power Modules, 2 Intelligence Modules, 4 SYBT5 Battery Modules |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

* 1. Nogales High School Data Center

| Rack | Equipment |
| --- | --- |
| Rack 1 | 5 Aruba 8310 POE (stacked Cisco switches) |
|  |  |
|  |  |
|  |  |

1. COMMUNICATIONS REQUIREMENTS

This appendix should include the most accurate data associated with the data and voice communications in place for district. It should include an inventory of all communications equipment, diagrams and uniquely identified data WAN and LAN circuits, data net-work backup alternatives, and voice network specifications.

**Insert Wide Area Network Diagram Below**

1. EXTERNAL SUPPORT AGREEMENTS

This appendix should include documentation for service and emergency maintenance agreements with manufacturers, data storage facilities, telecommunications providers, and staff transportation providers. It should include points of contact and authorization procedures for delivery of services.

1. DATA CENTER EMERGENCY PROCEDURES AND REQUIREMENTS

This appendix should include additional emergency procedures for all secured data center facilities. Information on fire, smoke, water, and intrusion alarms should be included. Power down procedures should be included. Facility layout, power requirements, cable diagrams, and media connection outlets should be included.

* Uninterruptible power supplies (UPS) provide short-term power to all systems to allow time for a graceful shutdown of systems that should minimize data loss. A UPS should be able to support the system for at least 30 minutes to one hour.
* Fire suppression system
* Fire and smoke detectors
* Water sensors in ceiling and
* Emergency master shutdown switch
* Frequent, scheduled backups
* Heat-resistant and waterproof containers for backup media
* Off-site storage location for backup media
* Redundant hardware.
	1. Data Center Startup and Shutdown

The purpose of this standard procedure is to establish procedures for manually shutting down and starting up servers and virtual machines in the district data center to ensure safe, graceful shutdown of critical systems. Following this procedure will help to prevent data loss or damage to network hardware.

* + 1. Shutdown Procedures

In the event of a power outage that causes the data center to lose power and necessitates a data center shutdown, the uninterruptable power system (UPS) will activate. The UPS will only temporarily provide power for approximately 5 hours and as a result, designated IT operations staff shall perform the following process steps if onsite during normal business hours or if possible as on call.

1. Monitor temporary power status to ensure servers can be manually shutdown within the time remaining.
2. Report the time remaining to the Information Technology Director.
3. Begin notifying staff of the impending data center shutdown.
4. Immediately after the sites have been notified if the impending shutdown, begin shutting down the servers in the order described in the Server Shutdown Order List.
5. **CAUTION**: ***Physical servers MUST be shutdown not just powered off.***
6. Virtual Servers – Virtual servers must be logged into and shutdown first unless specifically specified. To shut down a virtual server log into the server’s host and complete shutdown. Monitor completed shutdown in virtualization manager.
7. Physical Servers – To shut down, log into the server through KVM or remote utility such as ILO and complete shutdown.
	* 1. Server Shutdown Sequence:
8. Non-critical servers:
	1. Antivirus
	2. Password Reset
	3. Imaging Server
	4. NAS
	5. Non-production PowerSchool
	6. Network Sniffers for Copier/Printer Service
9. More important, but still not critical systems:
	1. User Data Storage - home drives/other
	2. HR-Personnel Database Server
	3. Windows Updating Server
	4. Textbook/Library Systems Server
10. Critical, Production Servers:
	1. Accounting
	2. Payroll
	3. Accounts Payable System & Databases - 5 servers
	4. Shutdown database servers prior to other Remote Desktop/Terminal Servers
	5. Time Keeping System - 2 servers
	6. E-Mail Archive
	7. Disk-to-disk backup system
11. Leave the most critical servers to shutdown last
	1. Shutdown Domain Controller Virtual Machines
	2. Virtual Machine Host
	3. Web Filter - 2 servers
	4. Network Monitoring
	5. Firewall
		1. Startup Procedures

Once power is restored to the data center and the power has been stable for at least 15 minutes, the data center will need to be started up again using the following process.

1. Begin notifying staff the power has been restored
2. Begin startup of the servers in the **reverse** order described in the Server Shutdown Sequence.
3. Verify system operations normal and stable. Notify staff once all clear
4. PLAN MAINTENANCE PROCEDURES

The Contingency Plan must be maintained in a ready state that reflects system requirements, procedures, organizational structure, and policies. Information systems frequently change due to shift of business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly as part of the organization’s change management process to ensure that new information is documented and contingency measures revised, if required.

The ADMINISTRATIVE MANAGEMENT TEAM will review the contingency plans for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements will require more frequent reviews, such as contact lists. At a minimum, plan reviews should focus on the following elements:

* Operational requirements
* Security requirements
* Technical procedures
* Hardware, software, and other equipment
* Team members names and contact information
* Alternate and offsite facility requirements
* Vital records (e.g., electronic and hardcopy)

Because the contingency plan contains sensitive operational and personnel information, its distribution should be marked accordingly and controlled. Typically, copies of the plan are provided to recovery personnel for storage at home and office. Additionally, a copy should also be stored at the alternate site in the event local plan copies cannot be accessed because of the disaster.

1. CONTINGENCY LOG

This appendix should include the assessments and results of any exercise or real contingency operations. It should be written from available documentation after recovery and restoration. Include comprehensive lessons learned documenting unanticipated difficulties, staff participation, restoration of system backups, permanent lost data and equipment, and shut down of temporary equipment used for the resumption, recovery, and restoration.

* 1. May 16, 2018 – 1:00 – 3:00 PM

Attendance

Alejandro Arellano

Carlos Bolivar

Aissa Bonillas

Angelina Canto

Gabriel Castillo

Juan Cervantes

Oscar Islas

Kevin Kuhm

Alex Lopez

Judith Mendoza

Cesar Miranda

Ernest Nicely

Adelmo Sandoval

Mariebeth Silva

Carlos Tavares

Alma Trujillo

Roxane Zepeda

Mayra Zuniga

Background and Review of Contingency Plan

Because this was the first time many of the committee had seen the completed Contingency Plan we provided a background for its creation and stepped through the plans different parts.

This plan was initiated by a recommendation from the Auditor General’s office. The District did not yet have a formal plan created. For the last 6 months to this point, information about the various systems and services has been gathered and compiled into this document. Various processes and team members have also been documented to address possible disasters or outages. Members of these teams along with other interested stakeholders were gathered today to formally review and comment on the finished draft.

During this part of the meeting various suggestions were made and the roles of each group were explained and clarified. These suggestions will be incorporated into the final draft of the plan prior to board presentation. And, as this is a working document, future suggestions will also be added as necessary.

Simulated Scenario – Internet Outage

To demonstrate the steps of the contingency plan we walked through a hypothetical situation similar to an actual situation from the spring of 2016. We assumed an Internet outage. In this scenario the actual cause of the outage is not immediately known.

The IT Systems Team recognizes the outage and notifies the Damage Assessment team as well as the administrators at the various schools. Once the cause of the issue is determined – in this case a malfunctioning firewall – further information is disseminated to the various administrators and the Damage Assessment team is gathered to review solutions and costs.

Once the solution is determined – replacement of the device – an ETA is communicated to the school and district administrators. The Configuration Management Team will work with the vendor to install and configure the new device. Once installation is complete the Communications Team will work with each school and the District Office to verify connectivity and access to resources.

Notes and Lessons Learned

There were two main lessons taken from this initial meeting:

1. The district must evaluate the costs of various proactive measures that could mitigate or prevent potential outages. Spare equipment, redundant services or local partnerships could shorten the durations of common issues or outages. These costs can be reduced by maintaining current aged equipment or through the use of funding sources such as E-Rate.
2. Each school and department must review or prepare their individual communication plans. Communication of issues or outages should propagate from the Damage Assessment Team or Administrative Management Teams to individual schools or departments who should then disseminate the information to their staff members. This method occurs now but must be reviewed at each level.
	1. July 23, 2019 – 2:00 – 3:30 PM

Attendance

1. NUSD Information Technology Services Log Monitoring
	1. NUSD IT will enable logging and auditing of systems for the purpose of identifying and preventing potential security risks. The following will be analyzed and reviewed as available and technically feasible:
* Failed and successful logins
* Modification of security groups
* Creation of new Active Directory Objects
* Account management activities including password changes (success and failure and account lockout)
* Group policy change
* anti-virus/anti-malware product
* Shares with critical data for the daily department operations
* Firewall logs will be monitored and reviewed for suspicious activity
* Content Web-Filter logs will be reviewed for attempts to access unauthorized/unwanted websites
	+ 1. The following information will be captured for each of the above items as feasible:
* Date and time of activity
* For connection logs: peer IP address
* Identification of user performing activity
* Description of attempted or completed activity
	+ 1. How resulting logs will be reviewed:
* Data will be collected using built in tools (Windows Event Viewer), manually by the Network Specialist and using third party tools (Gray Log product).
* Data will be collected from the Firewall
* Data will be collected from the Web Content Filter
* An internal security committee will meet periodically to review and analyze the resulting data
* Potential issues and high security risks will be identified and investigated
* Any findings or issues will be addressed and reported to the district administration or the appropriate authority
	+ 1. Data reviewers
* The internal security committee, formed by the IT Director and the Network Specialist will review the logs obtained from the different systems.
* The information will be forwarded to district administration or any other authority as needed.
* Information will also be forwarded to IT department network support for investigation and or analysis if appropriate.

* + 1. Frequency of review
* The internal security committee will meet once a month to review and analyze the logs.
* A sign-in sheet will be used as evidence of date and time of meeting and will be kept in a binder for future reference.

**NOGALES UNIFIED SCHOOL DISTRICT #1**

**Safety Guidelines for Power Strip and Extension Cord Use
Standard Operating Procedure (SOP)**

**Purpose:**

NUSD Safety Guidelines for Using Power Strips and Extension Cords is an internal standard operating technology department policy and defines a general process to encourage a safe electrical environment for staff, students, and equipment. This policy applies to all power strips and extension cords used at all NUSD facilities and to all employees, students, and outside vendors.

**Procedures:**

**How to Use Power Strips**

* Use only surge protectors or power strips that have an internal circuit breaker. These units will trip the breaker if the power strip is over loaded or shorted to prevent overheating.
* Restrict the use power strip use to low voltage electronics, such as computers, small clocks and lights.
* Plug power strips directly into permanently installed receptacles, i.e., outlets.
* Keep your power strip in a dry environment since electricity and water do not mix well. This involves being sure that your power strip is not near water or any other type of liquid.
* Any surge protector or power strip that does not have an internal circuit breaker, has frayed wires, or has a unit that is not working properly, should be reported to your immediate supervisor and should be replaced immediately.
* Visually inspect all surge protectors or power strips on a regular basis to ensure that they are not damaged or showing signs of degradation. During the visual inspection, ensure that the plug is fully engaged in its receptive outlet.

Note: A power strip is a multi-outlet adapter with a flexible cord-and-plug attachment and an over-current device (breaker). Some power strips have a master on/off switch and some have a surge suppressor.

**Basic Power Strips Don’ts**

* Never use power strips for applications requiring heavy loads, including heaters, refrigerators, shop equipment, microwaves and other large appliances.
* Do not use power strips in applications requiring constant loads.
* Avoid using power strips in applications or facilities where power is critical.
* Never use power strips outdoors, particularly during damp weather. Besides being exposed to moisture, power strips used outdoors can be subjected to bugs, dirt, debris and other elements that could get inside unused ports and result in failure.
* Do not “daisy chain” power strips where they are connected to other power strips or extension cords. This can result in result in overloads, causing damaged appliances/equipment or even fire.
* Never drill or staple power strips for mounting. Always use proper mounting procedures including tabs or hangers often molded into power strip housings.
* Power strips should never be nailed, stapled, or taped to a desk, wall, ceiling, baseboard, or another object.
* Do not run extension cords through walls, doorways, under carpets, ceilings or floors. If the cord is covered, heat cannot escape, which may result in a fire hazard.
* Never use a cord that feels hot or is damaged. Touching even a single exposed strand can give you an electric shock or burn.
* Never use extensions cords or power strips for space heaters, refrigerators, microwave ovens, or toaster ovens.

**Power Strips vs. Surge Protectors**

Often, people confuse power strips with surge protectors. While a power strip is simply an extension cord that consists of several outlets, a surge protector contains an additional element. This element is designed to clamp the surge, meaning that it can remove the surge so that electronic equipment are protected from power irregularities or voltage spikes. Surge protectors provide an additional layer of safety and protection and are good ideas for power-sensitive applications.

**Other Concerns and Warnings**

* Some power strips have a push button that trips automatically when a strip gets too hot for safe use.
* Power strips are not intended as a permanent substitute for a wall receptacle.
* Power strips should not be routed through ceilings, floors, walls or other openings.
* If a power strip feels hot when touched, promptly unplug it.
* Immediately discard any cord that shows physical damage, such as cracks, exposed wires or splices.
* Inspect your power strips for any knotted or wounded cord, keeping in mind that a power strip cord needs to lie straight while being used.
* Always use the correct type of power strip. Before buying a particular product, check to ensure that it is UL (Underwriters Laboratory) certified and meets safety standards.
* Be sure that a power strip with a long cord is not a tripping hazard and is longer than six feet.
* Do not place a rug over a power strip cord as this can eventually lead to wires breaking in the cord. These wires can over heat which can cause a smoldering fire. As this typically occurs at night, this situation is extremely dangerous.

Installing additional outlets and other types of electrical jobs should only be handled by a highly qualified, experienced and licensed electrician. Electrical inspectors are trained to properly use power strips and can point out the electrical risks as a result of their misuse. If you feel that you need to add new outlets or need any kind of assistance with power strips/and or electrical appliances, please contact the Support Services or Technology Departments.

