BURBANK UNIFIED SCHOOL DISTRICT

CYBERSECURITY GUIDE

Board Approved:
05/16/2019

TABLE OF CONTENTS

Cybersecurity Guide Change Requests

This document contains Burbank Unified School District's (BUSD) written Cybersecurity Guide (Guide). All changes to this document will be controlled and managed using the following document change control process:

1. A change request to this document will be submitted to the Director of IT and Education Support in writing.
2. The person(s) submitting the change will include their justification for and benefits of the change in their written request.
3. The Director of IT and Education Support will present all change requests to the Facilities and Technology Subcommittee for review.
4. The Facilities and Technology Subcommittee will review and approve or disapprove each change request.
5. All changes to this document will be recorded in the Document Control Change Log below.
6. Once a year, an updated Cybersecurity Guide document will be presented to the Board of Education for review and approval.

Cybersecurity Guide Document Change Control Log

Date of Change Request	Change Requested by	Requested Change	Change Description	Date FTS Approved	Date Change Implemented	Change Implemented By

Cybersecurity Guide Overview

1. INTRODUCTION

The Board of Education intends for Burbank Unified School District (BUSD) to adhere to the requirements of The Family Educational Rights and Privacy Act of 1974 (FERPA), The Children's Internet Protection Act (CIPA), The Children's Online Privacy Protection Act (COPPA), Student Online Personal Information Protection Act (SOPIPA), and California Assembly Bill No. 1584 for the safeguarding of sensitive information and the protection of minors. To accomplish this, BUSD has developed this Cybersecurity Guide (Guide), which applies to all BUSD employees and third-party providers who process, store, or transmit sensitive data for BUSD.

2. PURPOSE

The purpose of this Guide is to establish general guidelines for securing, managing, and operating the cyber/information security and technology infrastructure of BUSD. The objectives of this Guide will encompass the following:

- Ensuring the confidentiality, integrity, and availability of sensitive information.
- Protecting against anticipated threats or hazards to such information.
- Protecting against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any BUSD student or employee.

This Cybersecurity Guide shall:

- Describe the elements that constitute cybersecurity.
- Explain the need for cybersecurity to preserve the confidentiality, integrity, and availability of sensitive information and organizational assets.
- Specify the various categories of data, equipment, connectivity devices, and processes subject to the Guide.
- Document responsibilities of each employee and functional area.
- Use approved standards and guidelines to establish appropriate security levels.
- Explain the appropriate administrative, technical, and physical safeguards in place to protect informational assets against unauthorized access or use.
- Help preserve data integrity by establishing guidelines preventing the alteration, manipulation, or compromise of information.
- Provide standards for efficient and appropriate use of information resources.
- Ensure guidelines are in place for the ongoing availability of information assets.

3. RESPONSIBILITY AND REPORTING

The safeguarding of sensitive information is the responsibility of all BUSD employees, board members, and third-party providers, and all have specific roles and responsibilities in developing, implementing, and enforcing an effective Guide.

Board of Education

The Board of Education has the overall responsibility for oversight of BUSD's Cybersecurity Guide. This includes approval of management reports and annual review and approval of the Guide. On an annual basis the Board of Education will:

- Appoint an Information Security Officer, currently the Director of IT and Education Support.
- Approve the Guide, including the Information Security Risk Assessment, all written information security policies, the Business Continuity/Disaster Recovery Program, the Incident Response Program, and the Vendor Management Program at least annually and make any revisions or amendments as needed.
- Review and approve an annual report on the overall status of the Cybersecurity Guide.

Facilities and Technology Subcommittee

The Facilities and Technology Subcommittee (FTS) is responsible and accountable for:

- Reviewing Guide enhancements, new products, or security concerns.
- Assisting the Director of IT and Education Support in the development, implementation, adjustment, and maintenance of the Guide.
- Holding meetings bi-weekly and maintaining written minutes for each meeting.
- Reviewing the activities of all third-party service providers that have access to BUSD's sensitive information and technology systems.

Director of IT and Education Support

The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for Guide administration, including:

- Management and oversight of the Information Security Risk Assessment (ISRA), policy development, standards and procedures, testing, training, and security reporting processes
- Review of the Guide and annual submission of a written report to the Board of Education describing its overall status
- Performing periodic user access reviews
- Monitoring adherence to policies and procedures
- Reviewing system security reports
- Testing aspects of the Guide
- Monitoring the physical security environment
- Responding to a cyber/information security event

Network/Systems Analysts

The Network/Systems Analysts are responsible and accountable for network administration and maintenance, including:

- Development, implementation, and oversight of network documentation
- Network user access rights administration
- Employee and third-party authentication
- Firewall administration and monitoring
- Network and host operating system administration
- Application access and administration
- Remote access and administration
- Endpoint security software administration

- Encryption
- System logging and monitoring
- Network administration reporting

Employees
Employees are responsible and accountable for:
- Reviewing, understanding, and adhering to Guide requirements.
- Proper use of information systems resource under their direct control.
- Reporting information security concerns to the Director of IT and Education Support.

4. CYBERSECURITY GUIDE GUIDELINES

The Board of Education appoints the Director of IT and Education Support as the Information Security Officer and the responsible party for assessing risks for unauthorized transfer of sensitive information and implementing procedures to minimize those risks to BUSD. The ISO will assess the internal control structure put in place by BUSD and to verify that all BUSD departments adhere to the general requirements of these guidelines.

Facilities and Technology Subcommittee

1. INTRODUCTION

Burbank Unified School District (BUSD) has a responsibility to establish and maintain a Facilities and Technology Subcommittee (FTS). The Board of Education will appoint subcommittee members who represent a broad range of expertise and knowledge of BUSD's operations and functional areas.

2. PURPOSE

The purpose of this guideline is to communicate the FTS's purpose and responsibilities for the Cybersecurity Guide (Guide).

3. RESPONSIBILITY AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- Annual membership approval and oversight of the FTS.
- Review and approval of FTS minutes submitted to the Board.

Director of IT and Education Support
The Director of IT and Education Support will serve as the Information Security Officer (ISO) and is responsible and accountable for:

- Bringing all system logs and monitoring reports to the FTS for review.
- Reviewing network administration reports.
- Reviewing all IT security issues with the FTS.
- Reviewing any change requests with the FTS.
- Researching new technologies to discuss with the FTS.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Oversight of BUSD's cybersecurity activities; however, specific responsibilities may be distributed throughout BUSD as necessary. Key responsibilities of subcommittee members include:
  - Overseeing the Cybersecurity Guide.
  - Managing the information security risk assessment process.
  - Understanding the impact of technology on District operations.
  - Helping to define new processes and techniques and identify technical tools.
  - Identifying technology initiatives that will support strategic and educational plans.
  - Reviewing the need for specific technology initiatives.
  - Prioritizing technology projects and reviewing all technology requests prior to submitting to the Board of Education for approval.
  - Prioritizing training requirements to best utilize technology.

- Overseeing implementation of technology initiatives.

4. FACILITIES AND TECHNOLOGY SUBCOMMITTEE GUIDELINES

The FTS will:

- Be aligned with educational goals and objectives of BUSD and maintain a district technology plan.
- Approve and oversee the implementation of cybersecurity measures, including risk assessments, policies and procedures, and training.
- Review all cybersecurity audits and monitor all findings to resolution.
- Provide adequate reporting to management and the Board of Education regarding major cybersecurity initiatives and activities.
- Establish a sound methodology for review and approval of Guide projects.
- Review major cybersecurity and technology purchases and seek approval as required for such purchases.
- Maintain a business continuity/disaster recovery plan and incident response plan.
- Maintain written minutes of each committee meeting.
- Review staff training needs related to cybersecurity.
- Oversee the development and maintenance of cybersecurity policies and procedures.

Cybersecurity Strategy Guidelines

1. INTRODUCTION

Burbank Unified School District (BUSD) has the responsibility to develop, implement, and maintain an effective Cybersecurity Strategy to provide an overall framework for safeguarding BUSD's sensitive information. The strategy should provide the Board of Education with assurance that the proper controls and monitoring are in place to safeguard BUSD's sensitive information.

2. PURPOSE

The Cybersecurity Guide (Guide) policies will incorporate BUSD's Cybersecurity Strategy and establish clear guidelines for all personnel to maintain a controlled, secure, and productive technology environment. Information security will protect the confidentiality, availability, and integrity of BUSD's sensitive information assets.

3. RESPONSIBILITY AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- Guide oversight and annual review of the Cybersecurity Strategy.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Guide security administration and annual employee training.
- Review of the Guide and annual submission of a written report to the Board describing the overall status of the Guide.

Facilities and Technology Subcommittee
The FTS is responsible and accountable for:

- Guide oversight and the development, implementation, and maintenance of an effective Cybersecurity Strategy to develop and maintain the Guide.
- Communicating the Guide policies and establishing clear guidelines for all personnel to ensure they understand their responsibilities for safeguarding information.
- Establishing and maintaining an effective Information Security Risk Assessment (ISRA) and shall review and update it prior to any Guide changes and at least annually.
- Monitoring the roles and responsibilities of all third-party providers that have access to BUSD's sensitive information and technology systems. The FTS will contractually require that third-party providers implement appropriate security measures.

Employees

BUSD Employees are responsible and accountable for:

- The proper care, use, and safeguarding of BUSD's information and technology systems.
- Reading BUSD's Board Policy/Administrative Regulation 4040 and signing the Acceptable Use Agreement - Employee/Volunteers form to certify they understand this agreement.

4. CYBERSECURITY STRATEGY GUIDELINES

The Cybersecurity Strategy shall include:

- A Guide to mitigate foreseeable risks while complying with legal, contractual, and internally developed requirements. It will include relevant policies, standards, and procedures; information and technology systems architecture; physical security; resource dedication; training; and independent testing, reviews and audits.
- The implementation of layered controls for risk mitigation.
- Periodic updates as changes occur in BUSD's risk environment.
- An annual report to the Board of Education on the overall status of the Guide.

Information Security Risk Assessment Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to develop, implement, and maintain an effective Information Security Risk Assessment Program. Key BUSD personnel shall participate in the risk assessment process to define the Cybersecurity Guide's (Guide) policies, guidelines, and controls.

2. PURPOSE

The Information Security Risk Assessment will assure the Board of Education that risks and threats to sensitive information and technology systems are properly identified, measured, monitored, and controlled. The Information Security Risk Assessment (ISRA) is an assessment of BUSD's technical and non-technical informational assets and the level of risk associated with those assets. The assets are risk weighted under the following categories:

- Threat - Events that could cause harm to the confidentiality, integrity, and availability of information or information systems. These events include: internal and external threats, human, natural, and technical.
- Vulnerability - Weaknesses in a system, or control gaps that, if exploited, could result in unauthorized disclosure, misuse, alteration, or destruction of information or information systems.
- Business Impact - Impact of potential threats or vulnerabilities on the confidentiality, integrity, availability, operations, and financials of BUSD.
- Probability of Occurrence - The probability or likelihood that threats or vulnerabilities could impact information given the current control environment.
- Controls - The controls used to mitigate threats and vulnerabilities decreasing the impact or probability of occurrence. These controls can be in the form of preventative, detective, and corrective measures.

The ISRA may be reviewed and updated periodically to reflect the current level of risk. The ISRA is submitted to the Board of Education at least annually for review and approval. All changes and updates are risk assessed prior to being implemented.

3. RESPONSIBILITY AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- Oversight of the ISRA and control decisions.
- Annual review and approval of the ISRA.

Director of IT and Education Support

The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Leading the Facilities and Technology Subcommittee in the development, implementation, and maintenance of the ISRA.
- The first ISRA shall be completed by June 30th, 2020.

Facilities and Technology Subcommittee (FTS)

The FTS is responsible and accountable for:

- The development, implementation, and maintenance of the ISRA

Employees

BUSD Employees are responsible for:

- Day-to-day assurance that sensitive information is afforded protection of information integrity, availability, and confidentiality.
- Review information security guidelines contained within this Guide and attend annual information security training.
- Report any information security concerns to the Director of IT and Education Support immediately.

4. INFORMATION SECURITY RISK ASSESSMENT GUIDELINES

The Director of IT and Education Support will ensure the guidelines, processes, and procedures listed below are implemented to support the development, maintenance, and ongoing support of BUSD's ISRA.

- The ISRA shall be updated after all Guide changes and at least annually.
- The ISRA process shall identify:
    - All Information Assets that store, transmit, or process sensitive information;
    - The Value of the Information Asset to BUSD's operations;
    - Reasonably foreseeable Risks to each Information Asset;
    - The Likelihood of the Risk occurring;
    - The Impact to BUSD's operations if the Risk occurs;
    - A calculation of the Inherent Risk of each Information Asset;
    - Relevant Controls to mitigate each Risk;
    - The Effectiveness of each Control;
    - A calculation of the Residual Risk of each Information Asset.
- The risk assessment process will consider the areas within BUSD to be assessed and the risk to sensitive information stored on both paper and electronic media. The assessment will also consider the controls needed to safeguard sensitive information from risks and threats.
- For those Information Assets with a Residual Risk greater than "Low," the risk assessment shall document additional controls to reduce the Residual Risk or shall document the Board of Education's acceptance of the higher risk level.
- The Inherent Risk ratings of each Information Asset shall be used to guide the scope and frequency of the Information Security Audit Program, where those Information Assets with a higher Inherent Risk level will be audited more frequently.

- The Director of IT and Education Support will report the outcomes of the annual information security risk assessment to the FTS and the Board of Education for review and approval.

Acceptable Use Agreement – Employee/Volunteer

The Burbank Unified School District authorizes district employees/volunteers to use technology owned or otherwise provided by the district as necessary to fulfill the requirements of their position. The use of district technology is a privilege permitted at the district's discretion and is subject to the conditions and restrictions set forth in applicable Board policies, administrative regulations, and this Acceptable Use Agreement. The district reserves the right to suspend access at any time, without notice, for any reason.

The district expects all employees/volunteers to use technology responsibly in order to avoid potential problems and liability. The district may place reasonable restrictions on the sites, material, and/or information that employees/volunteers may access through the system.

The district makes no guarantee that the functions or services provided by or through the district will be without defect. In addition, the district is not responsible for financial obligations arising from unauthorized use of the system.

Each employee/volunteer who is authorized to use district technology shall sign this Acceptable Use Agreement as an indication that he/she has read and understands the agreement.

Definitions

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

Employee/Volunteer Obligations and Responsibilities

Employees/volunteers are expected to use district technology safely, responsibly, and primarily for work-related purposes. Any incidental personal use of district technology shall not interfere with district business and operations, the work and productivity of any district employee/volunteer, or the safety and security of district technology. The district is not responsible for any loss or damage incurred by employees/volunteers as a result of their personal use of district technology.

The employee/volunteer in whose name district technology is issued is responsible for its proper use at all times. Employees/volunteers shall not share their assigned online

services account information, passwords, or other information used for identification and authorization purposes, and shall use the system only under the account to which they have been assigned. Employees/volunteers shall not gain unauthorized access to the files or equipment of others, access electronic resources by using another person's name or electronic identification, or send anonymous electronic communications. Furthermore, employees/volunteers shall not attempt to access any data, documents, emails, or programs in the district's system for which they do not have authorization.

Employees/volunteers are prohibited from using district technology for improper purposes, including, but not limited to, use of district technology to:

1. Accessing, posting, submitting, publishing, or displaying harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or unlawful discrimination, including discriminatory harassment, intimidation, and bullying, targeted at any employee or student by anyone, based on the employee or student's actual or perceived race, color, ancestry, nationality, national origin, immigration status, ethnic group identification, ethnicity, age, religion, marital status, pregnancy, parental status, physical or mental disability, sex, sexual orientation, gender, gender identity, gender expression, or genetic information, or association with a person or group with one or more of these actual or perceived characteristics. This includes political beliefs.

2. Disclose or in any way cause to be disclosed confidential or sensitive district, employee, or student information without prior authorization from a supervisor

3. Engage in personal commercial or other for-profit activities without permission of the Superintendent or designee

4. Engage in unlawful use of district technology for political lobbying

5. Infringe on copyright, license, trademark, patent, or other intellectual property rights

6. Intentionally disrupt or harm district technology or other district operations (such as destroying district equipment, placing a virus on district computers, adding or removing a computer program without permission, changing settings on shared computers)

7. Install unauthorized software

8. Engage in or promote unethical practices or violate any law or Board policy, administrative regulation, or district practice

Privacy

Since the use of district technology is intended for use in conducting district business, no employees/volunteers should have any expectation of privacy in any use of district technology.

The district reserves the right to monitor and record all use of district technology, including, but not limited to, access to the Internet or social media, communications sent or received from district technology, or other uses within the jurisdiction of the district. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Employees/volunteers should be aware that, in most instances, their use of district technology (such as web searches or emails) cannot be erased or deleted.

All passwords created for or used on any district technology are the sole property of the district. The creation or use of a password by an employee/volunteer on district technology does not create a reasonable expectation of privacy.

Personally Owned Devices

If an employee/volunteer uses a personally owned device to access district technology or conduct district business, he/she shall abide by all applicable Board policies, administrative regulations, and this Acceptable Use Agreement. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

The following guidelines shall be followed when using personally owned devices to access BUSD resources:

1. Confidential information shall not be stored on mobile devices.

2. Keep mobile device operating systems and applications up-to-date with the latest security patches and enable automatic updates.

3. Secure all mobile devices with a strong password and encryption when possible.

4. Install and maintain appropriate endpoint security protection on mobile devices.

5. Report any suspected incident of unauthorized data access immediately to the Director of IT and Education Support.

6. Refrain from forwarding sensitive BUSD information to personal email accounts or to non-BUSD employees.

7. Refrain from leaving mobile devices unattended.

8. Refrain from using mobile devices to text or email while driving.

9. Agree and acknowledge that BUSD will establish audit trails to monitor access to internal BUSD resources and to identify unusual usage patterns or other suspicious activity. Audit trails may be accessed, published, and used without notice.

10. Participate in required training.

Records

Any electronically stored information generated or received by an employee/volunteer which constitutes a district or student record shall be classified, retained, and destroyed in accordance with BP/AR 3580 - District Records, BP/AR 5125 - Student Records, or other applicable policies and regulations addressing the retention of district or student records.

Reporting

If an employee/volunteer becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of district technology, he/she shall immediately report such information to the Superintendent or designee.

Consequences for Violation

Violations of the law, Board policy, or this Acceptable Use Agreement may result in revocation of an employee's/volunteer's access to district technology and/or discipline, up to and including termination. In addition, violations of the law, Board policy, or this agreement may be reported to law enforcement agencies as appropriate.

Employee/Volunteer Acknowledgment

I have received, read, understand, and agree to abide by this Acceptable Use Agreement, BP/AR 4040 - Employee Use of Technology, and other applicable laws and district policies and regulations governing the use of district technology. I understand that there is no expectation of privacy when using district technology or when my personal electronic devices use district technology. I further understand that any violation may result in revocation of user privileges, disciplinary action, and/or appropriate legal action.

I hereby release the district and its personnel from any and all claims and damages arising from my use of district technology or from the failure of any technology protection measures employed by the district.

Personnel Name:_____ Position: _____
(Please print)

School/WorkSite: _____

Employee / Volunteer (Please Circle)

Signature:_____ Date:_____

Acceptable Use Agreement – Students

The Burbank Unified School District authorizes students to use technology owned or otherwise provided by the District along with personal devices for instructional purposes. The use of technology while on campus is a privilege permitted at the District's discretion. It is subject to the conditions and restrictions set forth in applicable Board policies, administrative regulations, and this Acceptable Use Agreement.

The District expects all students to use technology responsibly in order to avoid potential problems and liability. The District may place reasonable restrictions on sites, materials, and/or information that students may access through our system. The District uses technology protection measures to block or filter access, as much as reasonably possible, to visual and written depictions that are obscene, pornographic, or harmful to minors over the network. The District can and will monitor users' online activities and access, review, copy, and store or delete any communications or files and share them with adults as necessary. Users should have no expectations of privacy regarding their use of district equipment, network, and/or internet or files, including email. The above includes any and all personal items used on campus.

With parent/guardian permission, the District will make student e-mail accounts available for all secondary students. Students will be allowed to send e-mails to other district accounts only. Student e-mail accounts will be able to receive e-mails from outside sources allowing students the ability to use educational software and reset passwords. E-mail accounts are provided at the discretion of the District and can be suspended and/or revoked at any time.

For the purpose of this agreement, technology includes, but is not limited to: computers, the District's network (including servers and Wi-Fi), the Internet, e-mail, USB drives, laptops, tablets, phones, and any other electronic device.

By signing the Acknowledgement of Rights and Responsibilities form in the Annual Parent Notification Packet, you acknowledge that you understand the following:

1. I am responsible for practicing positive digital citizenship. As a representative of this school, I will accept personal responsibility for reporting any misuse of the network to a teacher, administrator, or system administrator. In addition, I agree to the following:
    a. I will practice positive digital citizenship, including appropriate behavior and contributions on websites, social media, discussion boards, media sharing sites, and all other electronic communications, including new technology.
    b. I will be honest in all digital communication.
    c. I understand that what I do and post online must not disrupt school activities or compromise school safety and security.

2. I am responsible for keeping personal information private.

a. I will not share personal information about myself or others including, but not limited to, names, home addresses, telephone numbers, birth dates.
b. I will abide by all laws, the Student Acceptable Use Policy, the Student Bring Your Own Device Policy, and all District security policies.

3. I am responsible for my passwords and my actions on District accounts.
a. I will not share any school or District usernames and passwords with anyone.
b. I will not access the account information of others.
c. I will log out of unattended equipment and accounts in order to maintain privacy and security.

4. I am responsible for my verbal, written, and artistic expression.

5. I am responsible for treating others with respect and dignity.
a. I will not send and/or distribute hateful, discriminatory, or harassing digital communications, or inappropriate texts.
b. I understand that bullying in any form, including cyberbullying, is unacceptable.

6. I am responsible for accessing only educational content when using District technology or personal technology on the District's network.
a. I will not seek out, display, or circulate material that is hate speech, sexually explicit, or violent.
b. I understand that any exceptions must be approved by a teacher or administrator as part of a school assignment.
c. I understand that the use of the District network for illegal, political, or commercial purposes is strictly forbidden.

7. I am responsible for respecting and maintaining the security of District electronic resources and networks.
a. I will not try to bypass security settings and filters, including through the use of proxy servers to access websites blocked by the District.
b. I will not install or use illegal software or files, including copyright protected materials, unauthorized software, or apps on any District computers, tablets, smartphones, or other new technologies.
c. I will not access the Internet through a personal data plan or hotspot for either district or personal devices.
d. I will not use the District network or equipment to obtain unauthorized information, attempt to access information protected by privacy laws, or impersonate other users.

8. I am responsible for taking all reasonable care when handling District equipment.
a. I understand that vandalism in any form is prohibited.
b. I will report any known or suspected acts of vandalism to the appropriate authority.
c. I will respect my and others' use and access to District equipment.
d. If I have received a laptop tablet device to use at home, by accepting the possession of the device I agree to the following.

i. I understand that it is to be used for school work only and in accordance with the Student Acceptable Use Policy.
ii. I shall not sell, lease or otherwise grant anyone rights to the device.
iii. I shall adhere to the District's rules and regulations governing the use of the device and software and comply with all applicable copyright and other regulations regarding the software.
iv. I understand that I am responsible for any damage to the device. The District may request the device and software be returned at any time. Upon request by the District or termination of the agreement, I must return the device to the District, in the same condition as on the agreement beginning date, reasonable wear and tear excepted.
v. I agree to accept the device and software "as is." In no event shall the District be liable to me for my use of the device.
vi. I understand that in the event of theft, misuse or carelessness, the device will not be replaced. I understand that if loss or damage occurs while the device is in a car, at my home, or anywhere outside of a district building, I am responsible for any damage, and in case of theft, for filing an official police report and informing my school immediately. I will personally guarantee reimbursement of the replacement cost of the device to the District or I will make arrangements with my school to complete community service hours if the equipment is lost or damaged.

9. I am responsible for respecting the works of others.
   a. I will follow all copyright (http://copyright.gov/title17/) guidelines.
   b. I will not copy the work of another person and represent it as my own and I will properly cite all sources.
   c. I will not download illegally obtained music, software, apps, and other works.

10. Using the district's computing and network resources is a privilege and not a right, and any inappropriate use will result in loss of those privileges. The designated system administrator(s) (operating under the aegis of the Board of Education) will decide what appropriate use is, and their decision is final. The system administrator(s) may close an account at any time deemed necessary. The administration or staff of the district may request the system administrator deny, revoke, or suspend specific user accounts.

11. The district makes no warranties of any kind, whether express or implied, for the service it is providing. The district has no control over the Internet. The district will not be responsible for any damages suffered while on the computer network systems. These damages include, but not are not limited to loss of data or service interruptions caused by the systems or by user errors or omissions. Use of any information gathered from the network systems is at the user's own risk. The district specifically denies responsibility for the accuracy of information obtained through its network services.

12. The information service may occasionally require new registration and account information from you to continue the service. You must notify the information system of any changes in your account information.

BRING YOUR OWN DEVICE POLICY – STUDENT GUIDELINES

The following guidelines explain appropriate use of personally owned mobile devices by students. Please note that classroom teachers make the final decision as to whether or not devices will be allowed to be used in the classroom.

1. Students may possess or use personal electronic signaling devices on school campus provided that such devices do not disrupt the educational program or school activities and are not used for illegal or unethical activities such as cheating on assignments or tests or accessing inappropriate content.

2. The District assumes no responsibility for loss, theft, damage, or maintenance of student owned devices that are brought to school. Students are solely responsible for the security of their own devices.

3. Electronic signaling devices shall be turned off and kept out of sight during class time or at any other time as directed by a school district employee, except where deemed medically necessary or when otherwise permitted by the teacher or administration. No student shall be prevented from using his/her cell phone in case of an emergency, except where that use inhibits the ability of school district employees to effectively communicate instructions for the safety of students.

4. The District assumes no responsibility for data used by students on individual cell plans.

5. Use of electronic devices to record video, pictures, and/or audio (while on campus) is not permitted unless given specific permission by staff member.

6. Students are responsible for bringing fully charged devices to school. Devices cannot be plugged in and left in classrooms or other areas of the school. Teachers and staff are not responsible for devices left in classrooms or other areas of school. Teachers and staff have discretion to allow charging if they deem it to be appropriate.

7. Devices are subject to search by school administration and/or law enforcement when it has been suspected that they have been used in an unlawful manner or there is reasonable suspicion of wrongdoing; such as (but not limited to) cheating on tests, unauthorized recording (audio and/or visual). Otherwise, school district employees will not search a device without the express authorized consent of the student and the student's parent or legal guardian.

8. Students are not permitted to record images, media, or student work without prior consent and authorization from a school administrator or teacher.

9. High school students may use electronic devices during passing periods, nutrition, lunch, and after school provided that they are not oppositional to any of

the above policies. Middle school students are only permitted to use devices during class with staff members' permission.

10. Students may not use electronic devices in ways that would disrupt educational or other school activities.

11. Students cannot be required to use their own personal devices. The District expects that teachers will provide other tools for students to use (as required by instruction and equity of access) when personal devices are not available or students choose not to use them.

12. Students may not share their personal electronic devices (for classroom use).

Violations of these conditions may result in progressive discipline. If a student's use of an electronic signaling device causes a disruption, a school district employee, on the first offense, may direct the student to turn off the device or reprimand the student. On subsequent offenses, the employee may confiscate the device and return it to the student at the end of the class period, school day or activity. A student's right to carry such devices may be revoked for subsequent offenses except where deemed medically necessary. Students may be subject to other disciplinary measures when their use of an electronic signaling device violates independent school rules, such as prohibitions on cheating.

Business Continuity/Disaster Recovery Program Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to develop a comprehensive Business Continuity/Disaster Recovery Program (BC/DRP) to provide for the continuation of daily operations and to provide educational services in a safe, secure, and reliable manner.

2. PURPOSE

These guidelines apply to BUSD's critical functions and daily operations of the technology infrastructure. The BC/DRP is comprised of a series of departmental and functional area plans and structured to enable BUSD to recover operations efficiently and effectively, and with the flexibility to respond to different events with differing levels of severity and complexity. For detailed procedures, see the Business Continuity/Disaster Recovery Plan.

3. RESPONSIBILITY AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- Approving annual updates to the BC/DRP.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Leading the Facilities and Technology Subcommittee in the development, implementation, and maintenance of the BC/DRP.
- Declaring whether a business disruption is considered a disaster.
- The initial BC/DRP shall be completed by June 30th, 2021.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Overseeing activities of the Business Continuity/Disaster Recovery Team (BC/DR Team).
- Prioritizing, reviewing, and approving resource requirements needed to develop and maintain the BC/DRP, including the Business Continuity/Disaster Recovery Risk Assessment, Business Impact Analysis, and resumption plans for critical functions.
- Annual review of a summary of BC/DRP test results.

Business Continuity/Disaster Recovery Team Leader

The Business Continuity/Disaster Recovery Team Leader (BC/DR Team Leader) is responsible and accountable for:

- Overseeing activities of BC/DR Team customers as directed.
- Providing support and coordination of the overall BC/DRP.
- Ensuring backup plans remain adequate.
- Scheduling and coordinating BC/DRP testing and training.
- Managing the execution of resumption efforts and directing recovery activities.
- Ensuring annual training and awareness programs are conducted.

Business Continuity/Disaster Recovery Team

The Business Continuity/Disaster Recovery Team (BC/DR Team) is responsible and accountable for:

- Meeting as needed to work on and discuss contingency activities.
- Planning for and reviewing BC/DRP adjustments.
- Reviewing and updating the BC/DRP and providing feedback to the FTS on risk mitigation strategies.
- Reviewing overall resumption plans for critical functions to ensure they can be restored within reasonable timeframes.

Employees

Employees are responsible and accountable for:

- Understanding the procedures for recovery of critical functions.
- Participating in periodic BC/DRP training and testing activities as assigned.

4. BUSINESS CONTINUITY/DISASTER RECOVERY PLANNING GUIDELINES

The FTS will ensure the BC/DR guidelines below are developed, implemented, and maintained to ensure safe, secure, and continued educational operations.

- The Director of IT and Education Support will develop, implement, and maintain an adequate Business Continuity and Disaster Recovery Plan. The plan will be tested annually.
- The FTS shall establish a BC/DR Team to develop, implement, maintain, and test the BC/DRP. The BC/DR Team Leader will identify participants to assist in this process.
- The goal of the BC/DRP will be to minimize data loss and impact, and ensure the availability of critical systems, personnel, and resources in the event of a system outage. The BC/DRP will ensure the continuity of critical functions and provide for rapid recovery to reduce the overall impact of a disaster.
- The BC/DRP will include defined roles and responsibilities of each individual involved with the contingency plan.
- The BC/DRP will identify BUSD's critical systems and include priorities for restoring these systems. BUSD's critical systems include:
    - Data Center HVAC and Fire Suppression Systems
    - Data Center Networking and Communication Systems
    - Data Center Compute and Storage Systems

- The Director of IT and Education Support shall test all critical systems at least annually, update the BC/DRP as necessary, and report test results to the Board of Education.
- The Director of IT and Education Support shall distribute copies of the plan and shall maintain copies in multiple locations. Copies of the plan will also be maintained at the residences of key BUSD personnel in the event of a disaster that occurs outside of normal business hours.
- The Director of IT and Education Support shall communicate the BC/DRP requirements and procedures to employees and training will be provided as needed.

Change Management Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to establish appropriate controls to mitigate risks or vulnerabilities introduced by changes to its information systems

2. PURPOSE

The Director of IT and Education Support shall establish adequate change control procedures to ensure the integrity of network devices, programs, and data. Change control procedures are necessary to establish adequate testing and recovery plans. These guidelines cover the following types of configuration changes:

- Installation of new computers
- Installation of new software applications
- New or updated operating systems
- Installation of patches and updates
- New technologies integrated with existing systems
- New policies, procedures, and standards
- New regulations
- New network devices
- Changes to the Wide Area Network (WAN)

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the Change Management Guidelines.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Oversight of BUSD's Change Management Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Authorization of work performed by third-party providers.
- Monitoring the status of all system testing and implementation.
- Review of all change management reports.

Network/Systems Analysts
The Network/Systems Analysts are responsible and accountable for:

- Automated system scans and patch deployment scheduling for Windows, macOS, iOS and Chrome OS operating systems.

- Coordinating with the Lead Technology Support Specialist on patch deployment and upgrades for third-party software (Adobe Reader, Adobe Acrobat, Adobe Flash Player, Oracle Java).
- Monthly reporting of applied system updates.
- Performance of critical changes and projects

.

4. CHANGE MANAGEMENT GUIDELINES

The Director of IT and Education Support will ensure the change management guidelines below are developed, implemented, and maintained to ensure the security of BUSD's information systems

- The Director of IT and Education Support shall develop baseline system and equipment configurations and install processes for new installations.
    - Workstation / Server Configuration Standards

      The installation of a new workstation and servers will consider the following baseline standards:
        - All unneeded services will be removed.
        - All up-to-date software patches and service packs will be applied.
        - Guest accounts will be disabled.
        - Rename the local administrator account
        - Limit the local administrator accounts to IT staff.
        - Install endpoint security software and current signature files
        - Enable the workstation firewall.
        - Enforce password policies and account lockout policy
        - Restrict physical access (servers).
- Network/Systems Analysts shall submit a change management request to the Director of IT and Education Support for major changes to system configuration.
- Network/Systems Analysts shall ensure that all network systems are properly backed up prior to the implementation of significant system updates or changes.
- The Network/Systems Analysts shall test LAN/WAN network configuration changes prior to introduction into the production environment when possible.
- The following five steps shall be performed as part of the patch management process:
    - Auditing: Audit of all applications to identify program/file name, version, and quantity.
    - Notification: The Network/Systems Analysts shall subscribe to sources such as US-CERT.gov for alerts on newly confirmed software vulnerabilities.
    - Patch Approval: The Lead Technology Support Specialist and Network/Systems Analysts shall verify software vendors and approve updates.
    - Automatic Patching: The Network/Systems Analysts shall apply patches via industry-standard enterprise management software.
    - Manual Patching: The Technology Support Specialists shall apply patches manually as directed by the Director of IT and Education Support.
- The Director of IT and Education Support will ensure that systems outsourced to critical service providers align with these guidelines.

Data Backup and Recovery Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to develop and maintain effective Data Backup and Recovery Guidelines to to ensure the confidentiality, integrity, and availability of its information systems.

2. PURPOSE

The Director of IT and Education Support will determine those systems where data backup and recovery guidelines and controls are implemented and maintained to provide for the management of proper backup of critical data and information.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the Data Backup and Recovery Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Providing oversight of BUSD's Data Backup and Recovery Guidelines.
- Ensuring that any storage facilities are practical and maintain a safe distance from BUSD
- Ensuring that access to backup media is limited to authorized personnel
- Ensuring that a written inventory of BUSD's critical electronic data is developed and maintained. The inventory should include a description of the data and where the data is physically stored and will serve as a guide as to what data needs to be included in backup procedures.

Network/System Analysts
The Network/Systems Analysts are responsible and accountable for:

- Periodically testing the backup restoration process.
- Ensuring all backups have been completed and recorded, and that all related media is secure.
- Ensuring that complete system backups are created when changes are made to the network operating system.

4. DATA BACKUP AND RECOVERY GUIDELINES

The Director of IT and Education Support will ensure the data backup and recovery guidelines below are developed, implemented, and maintained to ensure critical data and information can be recovered and restored.

- The Network/Systems Analysts will develop written procedures for the backup, testing, and restoration of each critical system and data source, and will determine the appropriate backup media for each critical system and data source.
  - Firewall and Content Filter Configurations
  - Switch and Router Configurations
  - VoIP Servers and Appliances
  - Blade Chassis Configurations
  - Domain Controllers and DNS Services
  - Radius Services
  - DHCP Services
  - Database Backups
  - File and Applications Servers
- All backup media will be clearly identified.
- Backups will be redundant, with at least one copy stored offsite to protect critical data and information in the event the primary site is involved in a disaster.
- Backups will be encrypted when transferred across the network
- Any individual backup media will be stored in a secure area and access to the backup media will be restricted to only those individuals responsible for the backup media.
- The Network/Systems Analysts will ensure that backup procedures are completed on the frequency defined by written procedures and will also maintain and review backup logs.
- The Director of IT and Education Support will ensure that systems outsourced to a service provider align with these guidelines.

Data Classification Guidelines

1. INTRODUCTION

The Data Classification Guidelines describe the responsibilities and processes Burbank Unified School District (BUSD) has developed to ensure the proper level of confidentiality, integrity, and availability protections are applied for sensitive data in the most cost-effective and efficient manner.

2. PURPOSE

The purpose of these guidelines are to identify and classify the information processed on BUSD systems and to establish controls for each information category for which BUSD is responsible. Data classification is a basis for establishing a baseline set of security controls for the information and information systems.

The categories are based on the potential impact to BUSD should the information be compromised. The classification system will be used to support incident response and business continuity/disaster recovery planning.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the Data Classification Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Performing annual audits of data classification.
- Implementing controls to protect confidentiality, integrity and availability of all data.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Oversight of BUSD's Data Classification Guidelines.

4. DATA CLASSIFICATION GUIDELINES

Director of IT and Education Support will ensure the data classification guidelines below are developed, implemented, and maintained to ensure critical data and information is maintained and secured appropriately.

Data Lifecycle

The data lifecycle is the series of stages data goes through in the course of its presence within the organization. BUSD uses a four-stage data lifecycle to describe the various stages of information on the network.

Acquisition
When BUSD creates information, it is in the Acquisition stage. System and business process metadata are assigned during the Acquisition stage. The data is also indexed to facilitate searching and assigned to the appropriate data store(s). Policy controls are applied to protect and restrict access of sensitive data. If necessary, roll-back capability is provisioned.

Use
After information is prepared and stored, it will be read and modified by BUSD users. During this stage, confidentiality, integrity, and availability are critical. Changes are mapped to the appropriate policies, regulations, or laws.

Archival
When information has reached a stage where it will no longer be actively used, it becomes archival data. Information may need to be retained for a variety of reasons, including legal and regulatory compliance. During this stage, additional controls are implemented on archival data to detect and protect it from unauthorized access or changes. Archival data will be backed up and encrypted based on its classification. The Data Assessment Program determines the appropriate retention period for archival data.

Disposal
The Data Classification Guidelines describe the method necessary to dispose of data when it is no longer necessary to retain it, as well as the entity responsible for the proper destruction of data prior to disposal.

Data Risk Rating

Security Objective	LOW	MODERATE	HIGH
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited adverse effec**t on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system	The disruption of access to or use of information or an information system	The disruption of access to or use of information or an information system could

	could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals.	could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.	be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.

Data Classification

After identifying all important data, BUSD classifies the data by sensitivity and criticality to quantify the loss that would be suffered if the information were lost. The Data Classification Level is stored in the metadata attached to all BUSD information assets. The Data Classification Level remains attached through the data lifecycle. Metadata is modified to reflect changes to the data that affect its classification to ensure proper protective controls are in place. Once data is segmented according to its classification, security controls are implemented to protect the data to an appropriate degree.

Data Classification Levels

BUSD utilizes four levels of classification for the organization's information. The sensitivity is determined based on the data usefulness, value, age, and level of damage that could be caused if the information were disclosed, modified, or corrupted. BUSD's data classification levels are also based on legal, regulatory, and contractual responsibility. All data is subject to classification, regardless of the form: digital, paper, video, fax, audio, etc.

Public: Public information is available or accessible to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public information is available to all BUSD parties and public disclosure will not cause an adverse impact. Loss of availability due to system downtime is an acceptable risk. Information integrity is important but not vital. Examples of public data include product brochures, information publicly available on website, newsletters, etc.

Sensitive: Sensitive information requires special precautions to ensure its integrity and confidentiality by protecting it from unauthorized modification or deletion. Sensitive information also requires higher than normal assurance of accuracy and completeness. Unauthorized access to sensitive information could affect BUSD's operational effectiveness, cause financial loss, or negatively impact student and community confidence. Information integrity is vital. Examples include Passwords and Security Policies, Process and Procedure Documents.

Private: Private information must be protected from unauthorized access, modification, transmission, storage, or other use based on to proprietary, ethical, or privacy considerations. This classification applies even though there may not be a civil statute requiring this protection. Private information is restricted to BUSD parties who have a legitimate purpose for accessing it. Examples include email, network information, private contact information, etc.

Confidential: Confidential information is protected by statutes, regulations, BUSD policies, or contractual language. Managers may also designate data as confidential. Confidential information is for use within BUSD only. Unauthorized disclosure could seriously affect the institution, its personnel, and its students. Confidential information may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside of BUSD should be authorized by the Superintendent or designee. Access to this information is very restricted. The highest possible levels of integrity, confidentiality, and limited availability is vital. All employees and contractors with access to confidential information will sign a Non-Disclosure Agreement prior to being granted access. The Superintendent must be notified in a timely manner if confidential data is lost or disclosed to unauthorized parties; suspected of being lost or disclosed to unauthorized parties; or is reasonably likely to have been lost or disclosed to unauthorized parties. The Director of IT and Education Support must also be notified in a timely manner if any unauthorized use of BUSD information systems has occurred, is suspected of happening, or is reasonably likely to happen. Examples include Personally Identifiable Information of Students and Employees, contracts, etc.

Data Classification Controls
BUSD requires the following controls based on the data's classification:

Storage
- Secured servers, computing devices or databases
- Access Control Administration Procedures for all levels of Sensitive, Private or Confidential Data and programs
- Encryption
- Auditing and monitoring
- Mobile Device Administration
- Locked file cabinets
- Periodic reviews of classification levels and controls
- Change control procedures
- Physical security protections
- Information flow channels
- Marking, labeling, and handling procedures
- Separation of duties
- Backup and recovery procedures

Transmission
- Encryption
- External emailing of unsecure confidential information is prohibited
- Use of email for sending/storing credit card numbers is prohibited

Distribution
- Only when authorized by Data Owner

Disposal and Destruction
- Data Destruction Guidelines

Responsibilities
All employees of BUSD have a responsibility to protect data from unauthorized generation, access, modification, disclosure, transmission, or destruction, and are expected to be familiar with and comply with these guidelines.

All employees are expected to familiarize themselves with these guidelines and to consistently use these standards when handling data. Although these guidelines provides overall guidance, to achieve consistent information protection employees are expected to apply and extend these concepts to fit the needs of operations. This document provides a conceptual model for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same classifications.

Data Owner
Data Owners are responsible for the protection and use of a specific subset of BUSD data. Data Owners are responsible for:

- Exercising due care for the data and responsibility for any negligent act that results in the corruption or disclosure of this data
- Classification of data under their protection
- Ensuring that the necessary security controls are in place for data under their protection

Data Custodian
The Data Custodian is responsible for:

- Maintaining and protecting data under their control
- Implementing and maintaining security controls
- Performing regular backups of data under their control
- Periodically validating the integrity of data under their control
- Restoring data from backup media
- Retaining records of activity involving data under their control
- Fulfilling the requirements specified in BUSD's security policy, standards, and guidelines that pertain to information security and data protection

System Owner
The System Owner is responsible for the systems that hold and process data owned by different Data Owners. System Owners are responsible for:

- Integrating application security considerations with purchasing decisions and development projects
- Ensuring that necessary security controls are implemented to protect data
- Assessing systems for vulnerabilities and reporting any to the Data Owner and he Director of IT and Education Support.

Director of IT and Education Support
The Director of IT and Education Support is responsible for:

- Implementing and maintaining specific security network devices and software in the enterprise. Examples include firewalls, intrusion detection systems, intrusion prevention systems, anti-malware, security proxies, and data loss prevention

- Ensuring access rights support the policies and Data Owner directives.
- Approving or rejecting requests to make changes to the network, systems, or software.
- Ensuring changes will not introduce any vulnerabilities.
- Ensuring proper testing of changes prior implementation in the production environment.

Management
Management is responsible for:
- Monitoring all user activity and any assets created and owned by these users
- Informing the Director of IT and Education Support of employee status changes to ensure subsequent access changes are realized

Network/Systems Analysts
The Network/Systems Analysts are responsible for:
- Ensuring data is stored appropriately
- Designing a system that will hold BUSD information
- Working with the Data Owners to ensure that the structures set up coincide with and support BUSD's objectives

Users/Employees
The Users are all of the individuals who routinely use the data for work-related tasks. Users are responsible for:
- Having the necessary level of access to the data to perform the duties within their positions
- Following operating security procedures to ensure the data confidentiality, integrity, and availability

Auditors (internal and external)
Auditors are responsible for:
- Periodically reviewing and confirming that the appropriate controls are in place and maintained
- Ensuring the organization complies with its own policies and applicable laws and regulations

Retention Policies
BUSD recognizes legal and regulatory requirements to ensure information is properly categorized for retention purposes. It also recognizes the need to ensure personnel adhere to these requirements. Retention Policies will be subject to regular documented audit procedures.

Protecting Information
Information Security Controls
BUSD shall place the following minimum controls on each information classification:
- Reproduction
  - Public – No restrictions on reproduction of public information are necessary.

    - Sensitive – Reproduction is authorized if not prohibited by the control statement.
    - Private – Reproduction is discouraged, however, if done, must be with permission from the owner or custodian.
    - Confidential – Reproduction is prohibited without permission of the owner or custodian.
- Distribution
    - Public – No restrictions on the distribution of public information are necessary.
    - Sensitive - Distribution shall be only to those who have a need-to-know and are either BUSD employees or a third party who has signed a non-disclosure agreement.
    - Private - Distribution must be only to those who have a business need-to-know and are either BUSD employees or a third party who has signed a non-disclosure agreement.
    - Confidential - Distribution must be only to those who have a stringent business need-to-know and are either BUSD employees or a third party who has signed a non-disclosure agreement.
- Electronic Mail (email)
    - Public – No email restrictions on public information are necessary.
    - Sensitive - May be sent to other BUSD employees or a third party who has signed a non-disclosure agreement.
    - Private - May be sent to other BUSD employees or a third party who has signed a non-disclosure agreement, but not over public networks unless protected by a BUSD-sanctioned encryption package.
    - Confidential - May only be sent internally, but not over public networks unless protected by a BUSD-sanctioned encryption package.
- Data Transmission
    - Public – No restrictions on data transmission are necessary.
    - Sensitive - Data transmission is authorized to other BUSD employees.
    - Private - Data transmission is authorized, but discretion should be used.
    - Confidential - Data transmission is prohibited unless encrypted by a BUSD-sanctioned encryption package.

Information Loss

Information loss can be divided into two potentially overlapping categories:

- Leakage
    - Sensitive information is no longer under the control of BUSD (loss of confidentiality) and often results from compromised databases, and its most common consequence is potential identity theft.
- Disappearance or damage
    - A correct copy of the information is no longer available to BUSD (compromise of integrity or availability).

Information Loss Prevention

Information loss prevention's goal is to protect sensitive information from leaving BUSD.

Loss Vectors

BUSD information exists in the following three major states.

- Information at rest: Residing in files systems, distributed desktops and large, centralized data stores, databases, or other storage methods.
- Information at the endpoint: Residing at the endpoints of the network such as laptops, USB devices, external drives, CD/DVDs, archived tapes and mobile devices.
- Information in motion: Moving through the network to the outside via email, instant messaging, peer-to-peer (P2P), File Transfer Protocol (FTP), or other communication mechanisms.

Information in each state requires different techniques for loss prevention. BUSD has developed an information loss prevention program to cover all the loss vectors the institution has the potential to encounter.

Solution Components

The Information Loss Prevention Program consists of the following components:

- Manage – BUSD information usage policies, reporting of information loss incidents, and establishment of incident response capability to enable corrective actions to remediate violations.
- Discover – BUSD has defined the sensitivity of information, created an inventory of sensitive information, located sensitive information wherever it is stored, and managed information cleanup. This includes sensitive information at rest in file servers, databases, documents and records management, email repositories, and web content and applications; and sensitive information stored on the endpoint including laptops, desktops, and workstations at remote offices to inventory, secure, or relocate that information.
- Monitor – BUSD monitors the use of sensitive information and understands usage patterns. BUSD monitors information in motion by inspecting network communications such as email, Instant Messaging (IM), web, File Transfer Protocol (FTP), Person to Person (P2P) and others for confidential data in violation of policy; and monitoring information at the endpoints such as downloading to local drives, copying to USB or other removable media devices, burning to CD/DVDs, and printing or faxing electronically.
- Protect – BUSD enforces security policies to secure and prevent sensitive information from leaving the organization. Controls protect sensitive information across endpoint, network, and storage systems. This includes protecting data-at-rest with automatic encryption, quarantine, and removal; restricting printing, saving, copying, accessing, movement and downloading of sensitive information to removable media or other drives; and stopping data-in-motion from being sent in violation of policy or encrypting information for secure exchange.

BUSD identifies all the potential information loss vectors in the organization and then prioritizes them based on criteria such as past breaches, volume of communications, volume of data, the likelihood of a breach, and the number of users with access to those vectors. BUSD focuses first on the most significant and highest impact areas and works to ensure information loss prevention efforts do not interrupt district activities.

Identification of Information Sources					
Information Source	Information Location	Controls Currently in Place	Data Owner	Data Custodian	Format

Email Retention Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to develop and maintain an effective Email Retention Guidelines to ensure the confidentiality, integrity, and availability of sensitive information transmitted and stored electronically.

2. PURPOSE

All emails are that are retained and managed by BUSD are legally required to be released in the event of a Public Records Act request or E-Discovery Request. In the past, the District has not formally adopted email retention guidelines, which means that all emails that exist on District email systems, including emails sent back in the 1990's, can be subpoenaed and the District is required to spend the time and resources to compile and release the requested emails. In order to reduce the unreasonable burden required to comply with record requests that can go back decades, the District will be implementing the following email retention guidelines for all employees.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the Email Retention Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Identifying and enforcing the appropriate email retention periods for all BUSD parties.
- Establishing procedures for notifying all BUSD parties of upcoming email deletion timeframes and ensuring information is deleted by those timeframes.
- Providing periodic reports on email retention status for all BUSD parties to the Facilities and Technology Subcommittee.
- Maintaining required email retention documentation for audit purposes.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Providing oversight of BUSD's Email Retention Guidelines and its requirements.

4. EMAIL RETENTION GUIDELINES

The Director of IT and Education Support will ensure the email retention guidelines below are developed, implemented, and maintained to ensure critical data and information can be provided in a timely fashion and within appropriate timeframes.

- Five-Year Email Retention
  - All students, teachers and staff will have a default five-year email retention policy. All emails older than five years will be automatically deleted.
- Ten-Year Email Retention Label
  - Cabinet Members (Directors and Assistant Superintendents) will have the standard five-year email retention policy but will also have the option to apply a retention label to an email folder to extend the retention to ten years for emails within that folder. This is to allow for compliance with federal or state programs that require up to ten years of email retention.
- Ten-Year Email Retention
  - The Superintendent, Board of Education, and Human Resources Department will have a default ten-year retention policy. For those individuals all emails older than ten years will be automatically deleted.

A date will be announced well ahead of time of when this new email retention guidelines will take effect so that all BUSD parties have ample opportunity to review older emails that will be subject to deletion. Any emails an affected party wishes to save for their personal records can be saved as a PDF by selecting the desired emails in Outlook and clicking File > Save as Adobe PDF. Each employee is for responsible for retaining records in accordance with their retention requirements if they must be retained beyond the 5 year retention period. Records that require permanent retention should not be stored in email and should instead be stored on your District provided cloud storage. If you need assistance, please open a help desk ticket by visiting https://support.burbankusd.org.

Encryption Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to develop and maintain effective Encryption Guidelines, procedures, and controls to ensure the security of its sensitive information and technology systems.

2. PURPOSE

These guidelines will document encryption requirements to protect sensitive information transmitted outside of BUSD's internal network. The use of encryption technology by BUSD will be limited to those specific areas of BUSD's technology infrastructure where encryption is required to secure sensitive information stored on electronic media or transmitted electronically.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the Encryption Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Training employees on the handling of sensitive information.

Network/Systems Analysts
The Network/Systems Analysts are responsible and accountable for:

- Implementing encryption technology on all systems that transmit sensitive information outside of BUSD's internal network.

4. ENCRYPTION GUIDELINES

The Director of IT and Education Support will implement the following encryption guidelines to secure sensitive information residing on electronic media or transmitted over data networks.

- The following systems and data will be encrypted:
  - Authentication data (i.e. passwords)
  - Backup media
  - Portable devices that may contain data classified as private or confidential (laptops, tablets, smartphones, USB drives, etc.)
  - Remote access connectivity/VPN
- Employees shall not electronically transmit sensitive information over unsecured networks without using approved encryption procedures.

- All email containing sensitive information transmitted outside of BUSD's networks must be encrypted.

Firewall Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to develop and maintain effective firewall policies, procedures, and controls to ensure the security of BUSD's information systems. These guidelines specifically cover BUSD's Internet firewall implemented to prevent unauthorized access to or from BUSD's internal network and the Internet.

2. PURPOSE

BUSD evaluates the risks involved in connecting to other networks and evaluates the use of the firewall internally and by third-party vendors to protect the integrity and security of its internal systems.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of BUSD's Firewall Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Ensuring that all periodic testing is conducted on BUSD's firewall(s).
- Ensuring the completion of external vulnerability/penetration testing and internal vulnerability/penetration testing.
- Ensuring controls are in place to restrict physical and electronic firewall access to authorized parties.
- Ensuring documentation detailing firewall configuration is accessible to authorized parties only.
- Evaluating the adequacy of software administration for the firewall used to protect BUSD systems and sensitive information from unauthorized traffic. Issues should address the following:
  - Firewall changes are documented by the change management process
  - Upgrades to compensate for known security weaknesses are provided and installed on a timely basis
  - Changes to firewall effectiveness are tested prior to implementation
  - Firewall operating system control features have been invoked
  - Firewall operating system default settings are adequate
  - Review periodic change management emails

Network/Systems Analysts
The Network/Systems Analysts are responsible and accountable for:

- Monitoring all firewall activity.
- Providing a weekly firewall activity report to the Director of IT and Education Support.
- Notifying the Director of IT and Education Support of emergency firewall events.
- Testing firewall patches and critical updates before applying.
- Maintaining logs of all firewall activity and reviewing on a periodic basis.

4. FIREWALL GUIDELINES

The Director of IT and Education Support shall develop, maintain, and implement the following firewall guidelines to safeguard BUSD's information systems.

- BUSD shall require the use of a firewall at all external entry points into its network. All internet traffic that leaves or enters BUSD travels through the firewalls.
- All firewalls are physically secured from the public.
- Network/Systems Analysts shall configure the firewall to support Network Address Translation (NAT) and to repel common attacks.
- The Director of IT and Education Support shall review any firewall changes with Network/Systems Analysts, unless the change requires immediate action.
- The firewall will only allow internal network traffic to the Internet over approved ports and/or application signatures.
- The firewall will block all traffic from the Internet to BUSD's internal network unless explicitly allowed over approved ports and/or application signatures.
- The firewall will create a demilitarized zone (DMZ) to segregate and control traffic between internal networks and servers that are accessible from the Internet.
- BUSD shall purchase and maintain the firewall manufacturer's annual maintenance contract.
- Administrative access to the firewall shall be limited to the Network/Systems Analysts and the Director of IT and Education Support.
- The firewall shall be tested by a reputable independent third party as part of BUSD's ongoing security Information Security Audit Program. External vulnerability/penetration tests shall be completed at least annually. An independent third-party shall provide a report of the external vulnerability/penetration test findings, and the Director of IT and Education Support shall document remediation in a timely manner.

Incident Response Program Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to establish a comprehensive Incident Response Program to prevent and address unauthorized access to sensitive information maintained by the district or its service providers that could result in substantial harm or inconvenience to affected parties.

2. PURPOSE

The purpose of these guidelines is to implement appropriate response procedures for designated BUSD personnel to prevent and address incidents of unauthorized access to or use of sensitive information and to notify affected parties as required. An "incident" is an act violating an explicit or implied security policy. A "breach" is the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." (§1798.82(g))

3. RESPONSIBILITY AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the IRP Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Monitoring the safeguards in place to protect internal systems from unauthorized attempts to access or use sensitive information.
- Timely notification to individuals affected by an incident involving their sensitive information when appropriate.
- Ensuring that all agreements with third-party providers require them to notify BUSD and to take appropriate action to address incidents of unauthorized access to sensitive information.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Annually reviewing the IRP Guidelines.
- Establishing an Incident Response Team (IRT) to execute the IRP.
- Activation of the IRP and the IRT upon notification of an incident.
- Understanding the safeguards in place to protect internal systems from unauthorized attempts to use sensitive information.

Incident Response Team
The Incident Response Team (IRT) is responsible and accountable for:

- Coordination of incident response procedures upon activation.

Employees
Employees are responsible and accountable for:
- Awareness of information security policies and procedures for protecting sensitive information.
- Reporting incidents of unauthorized access to sensitive information immediately to the Director of IT and Education Support.

4. INCIDENT RESPONSE GUIDELINES

The following procedures should be followed when BUSD suspects or becomes aware of an intrusion or unauthorized access to sensitive information. Throughout the entire course of the incident handling process, confidentiality of the investigation must be maintained among those involved.

BUSD's IRP shall contain the following procedures:
- Preparation for an Incident
- Identification of the Incident
- Assessment of the Incident
- Containing and Controlling the Incident
- Recovery from the Incident
- Notification of Federal and State Regulators and Law Enforcement
- Notification of Third-Party Vendor(s)
- Affected Party Notification
- Post-Incident Assessment

Preparation for an Incident:
BUSD's IRP shall include procedures for preparation for an incident, including establishing an incident response team and defining what constitutes an incident.

Identification of the Incident
BUSD's IRP shall include procedures for identification and assessment of the nature and scope of an incident, including the identification of what sensitive information systems and types of sensitive information have been accessed or misused.

1. The Director of IT and Education Support shall determine if the event is a real incident. Steps taken include, but are not limited to:
   - A review of the various systems' exceptions/security logs
   - A determination of the systems affected, damaged, copied, or corrupted.
   - If the event is an incident, terminate the current intrusion if ongoing and document the incident.
2. If the Director of IT and Education Support determines an incident has occurred, he will activate the IRT.
3. The FTS shall require that third-party providers take appropriate actions to address incidents of unauthorized access to BUSD's sensitive information, including prompt notification of an incident.

Assessment of the Incident

1. The IRT will record what action was performed, when it was performed, and who witnessed the action being performed.
2. The IRT shall assess the nature and scope of the incident and identify what sensitive information systems and types of sensitive information have been accessed or misused. The IRT will use the Information Security Risk Assessment to determine the nature of the information accessed, which will guide BUSD in responding to the incident.
    - The IRT will evaluate security logs in an attempt to understand how the person gained access to the system, as well as the information they accessed.
    - The IRT will document whether the system was left in production, was taken offline and is being analyzed, is offline and ready to be restored to production, or is replaced by another system. The information documented will include what was done, the exact time that it was done, who performed each step, and who witnessed each step. This information will be included in a formal post-incident management report.

Containing and Controlling the Incident

Based on the nature of the incident, the Director of IT and Education Support and Network/Systems Analysts will take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of sensitive information, including:

1. Eliminating the method of unauthorized access on all systems by:
    - Deactivating unnecessary services
    - Removing /placing additional security controls on third-party network access
    - Reconfiguring firewalls
    - Installing necessary software updates
    - Changing user passwords
    - Enforcing strong password practices
2. Securing all logs, audits, notes, documentation, and any other evidence gathered during the incident to establish the “chain of custody” for potential legal action.
3. Securing and monitoring affected user accounts and information.

Recovery from the Incident

Recovering from an incident essentially involves restoring systems to a known good state or returning processes and procedures to a functional state.

1. Determine the course of action relative to the incident.
2. Test affected systems or procedures prior to implementation.

Notification of Federal and State Regulators

The Director of IT and Education Support shall notify Multi-State Information Sharing & Analysis Center (MS-ISAC) Computer Emergency Response Team (CERT) as soon as possible after the identification and preliminary assessment of a security breach, including steps to notify law enforcement. The IRT will assist the Director of IT and Education Support in assessing the effectiveness of the IRP and in determining whether to notify affected individuals.

- Multi-State Information Sharing & Analysis Center (MS-ISAC) Computer Emergency Response Team (CERT)
    - 866-787-4722
    - soc@cisecurity.org
- California Department of Justice - Submit a Data Security Breach Form
    - https://oag.ca.gov/privacy/databreach/report-a-breach

Notification of Law Enforcement

The Director of IT and Education Support shall notify appropriate law enforcement immediately by telephone if the incident involves a Federal criminal violation requiring immediate attention.

- Burbank Police Department
    - (818) 238-3000
- Federal Bureau of Investigation
    - https://complaint.ic3.gov/

Notification of Third-Party Vendors

If the incident involves any unauthorized disclosure of a third-party vendor's software access related controls, documentation, or use of their software, the Director of IT and Education Support will direct the notification of the potential impact to the third-party vendor.

Notification of Affected Individuals

If the IRT determines the incident has or reasonably could result in the misuse of sensitive information and that notification will not interfere with an ongoing BUSD or law enforcement investigation, the Board of Education shall begin notifying affected individuals as soon as possible. However, if the Board of Education cannot determine specific individuals affected, it shall notify all potentially affected individuals as reasonably possible.

- Content of Notice
    - Notice will be given in a clear and conspicuous manner and will contain the following information:

      (A) The name and contact information of the reporting person or business subject to this section.

      (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

      (C) If the information is possible to determine at the time the notice is provided, then any of the following:
        - (i) the date of the breach,
        - (ii) the estimated date of the breach, or
        - (iii) the date range within which the breach occurred. The notification shall also include the date of the notice

      (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

      (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of [§1798.82(h)].

- Delivery of Notice
  - BUSD will also send notice via the following methods:

    (1) Written notice.

    (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

    (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information."

Post-Incident Assessment

- The IRT will brief the FTS and the Board of Education on the incident, including what happened, the cause of the incident, the resolution of the incident, and how BUSD can prevent the incident from reoccurring in the future.

Information Access and Authentication Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to define the responsibilities for authorizing access to its information systems to ensure the security of sensitive information.

2. PURPOSE

The BUSD shall implement access controls to sensitive information systems to permit only authorized individuals to access the information, and to protect the integrity and security of its information systems.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- Annually reviewing and approving the Information Access and Authentication Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Developing, maintaining, and implementing appropriate information access and authentication guidelines to provide or restrict access to BUSD's information systems.
- Authorizing system access for all users.
- Overseeing administration of network user access.
- Performing and documenting annual reviews of employee access to BUSD systems.

Network/System Analysts
The Network/System Analysts are responsible and accountable for:

- Performing the role of system administrator.
- Adding, changing, and removing employee system access.
- Implementing, monitoring, and reviewing system controls.
- Reviewing access violation incidents.
- Ensuring that employee PCs are configured with a password-protected screensaver and a 45 minute timeout provision.
- Removing system security access for terminated employees.
- Adding, changing, and removing network access for employees.
- Re-enabling locked network accounts for employees who have exceeded the maximum number of valid login attempts.

Human Resources
Human Resources is responsible and accountable for:

- Immediately notifying the Network/Systems Analysts in the event of change of employee status or termination of an employee to provide for prompt change or removal of logon IDs.

Employees
Employees are responsible and accountable for:

- Storing passwords securely.
- Never revealing passwords to anyone without the Director of IT and Education Support's verbal authorization.
- Adhering to BUSD password complexity requirements.
- Notifying the Director of IT and Education Support if a network or critical application account has been compromised.
- Notifying the Network/System Analysts if a network or critical application account has been locked.
- Reporting unauthorized usage of BUSD's equipment to Director of IT and Education Support.
- Setting a unique password for their BUSD Active Directory account and locking their PCs (Ctrl-Alt-Del) when leaving their work area.

4. INFORMATION ACCESS AND AUTHENTICATION GUIDELINES

Active Directory (Network)

- The Network/System Analysts shall add new users, assign and change user access levels, and disable terminated users.
- The Director of IT and Education Support shall perform annual user access reviews.
- Guest and generic account usernames and passwords shall be changed or disabled.
- Administrative access rights shall be limited to the Network/System Analysts and Director of IT and Education Support.
- Users shall be required to have a unique username and password to access the network. Multiple users shall not use the same account to access the network.
- Users shall lock their PCs when leaving their work area.
- Passwords shall be at least 8 alphanumeric characters.
- Password complexity shall be enforced and shall require all of the following:
  - Uppercase letter
  - Lowercase letter
  - Number
  - Special Character
- The Password History is 1 passwords remembered.
- The Minimum Password Age is 0 days.
- The Maximum Password Age is 2 years.

OTHER SYSTEM(S)

- The Network/System Analysts shall add new users, assign and change user access levels, and disable terminated users.
- The Director of IT and Education Support shall perform annual user access reviews.
- Guest and generic account usernames and passwords shall be changed or disabled.
- Administrative access rights shall be limited to the Network/System Analysts and Director of IT and Education Support.
- Users shall be required to have a unique username and password to access the network. Multiple users shall not use the same account to access the network.
- Users shall set a password-protected screensaver and lock their PCs when leaving their work area.
- Passwords shall be at least 8 alphanumeric characters.
- Password complexity shall be enforced and shall require all of the following:
  - Uppercase letter
  - Lowercase letter
  - Number
  - Special Character
- The Password History is 1 passwords remembered.
- The Minimum Password Age is 0 days.
- The Maximum Password Age is 2 years.
- A user is automatically disabled after 5 invalid network access attempts and shall be required to contact BUSD Technology Help Desk to re-enable the account.

Password and Security Parameters

Password and Security Parameters	Active Directory	Other Systems
Minimum length of password	8 characters	8 characters
Password complexity* enforced	Yes	Yes
Maximum password age	2 years	2 years
Minimum password age	No	No
Retain password history	Yes, 1	Yes, 1
Number of unsuccessful sign on attempts allowed before account is “suspended” or “locked out”	N/A	5
Period of time that account is "locked out" after designated unsuccessful sign on attempts	N/A	Until BUSD Technology Help Desk resets

**Requires any three of the following: 1) capital letter 2) lowercase letter 3) number 4) special character*

Information Security Audit Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to support an Information Security (IS) Audit process to independently examine and evaluate BUSD's information security activities. Effective IS audit programs are risk-focused, promote sound controls, ensure the timely resolution of audit deficiencies, and inform the Board of Education of the effectiveness of risk management practices.

2. PURPOSE

The purpose of the IS Audit process is to provide independent, objective assurance of control effectiveness and to bring a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of BUSD's IS Audit Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Ensure that testing is conducted according to these guidelines.
- Provide testing results to the Facilities and Technology Subcommittee.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Identifying the inherent level of each BUSD information asset and establishing the appropriate test scope and frequency based on the information asset's inherent risk level.
- Reviewing the qualification of testing personnel to ensure they are capable of adequately supporting test objectives.

4. INFORMATION SECURITY AUDIT GUIDELINES

The FTS and Director of IT and Education Support will implement the following guidelines to develop, implement, and maintain BUSD's information security audit program:

- BUSD information assets shall be audited according to their inherent risk level. Higher-risk systems will be tested more frequently (i.e. annually). Additional factors to consider are the nature, extent, and results of prior tests; the value and

sensitivity of data and systems; and the occurrence of material changes to systems, policies, personnel, or third-party providers.

- IS audits may be outsourced to ensure the adequacy of independence and expertise. An engagement letter will be required by the vendor outlining the scope, responsibilities, and cost of the audit. Audit reports will be issued to the FTS to report significant audit findings.
- Components of the IS Audit program include:
  - Information Security Program Review
  - IT General Controls Review
  - External Vulnerability/Penetration Assessment
  - Internal Vulnerability/Penetration Assessment
  - Social Engineering Assessment
- BUSD shall contractually require third-party providers to implement appropriate measures to protect sensitive information. Third-party providers shall also be required to sign nondisclosure and confidentiality agreements.
- The Director of IT and Education Support shall track all test results to resolution and shall provide periodic status updates to the FTS.
- The Director of IT and Education Support shall ensure that critical systems or services outsourced to third-party providers are tested according to BUSD's guidelines. The Director of IT and Education Support will monitor the third-party providers' security testing by obtaining and reviewing independent audit and testing reports (i.e. SSAE 18 SOC 2 Type II reports, etc.).
- The FTS will determine the type and level of testing that is completed to validate BUSD's security control objectives are being met. Current testing schedule:
  - Full information systems general controls review every 24 months.
  - Audit of high-risk systems every 12 months.
  - External (Internet) vulnerability/penetration testing every 12 months.
  - Internal network vulnerability/penetration testing every 12 months.
  - Social Engineering assessments every 12 months.
- Test results that indicate an unacceptable risk to BUSD's information or technology systems will be tracked in writing and will include actions taken by management to reduce the risk to an acceptable level.
- Testing will encompass systems in BUSD's production environment and those systems within BUSD that provide access to the production environment.
- The FTS and the Director of IT and Education Support will review the qualifications of testing personnel to ensure the capabilities of testing personnel are adequate to support test objectives.

Malicious Code Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to establish appropriate protection of its network and sensitive information from malware. Malware (i.e. computer virus, spyware, SPAM, logic bomb, Trojan, worm, etc.) is software designed and installed on a network system or computer for a harmful purpose.

2. PURPOSE

These guidelines will document the controls in place to prevent, detect, and eradicate malware. Malware protection has been installed on all BUSD network and communications systems to ensure the confidentiality, integrity, and reliability of sensitive customer information and BUSD operations.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the Malicious Code Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Providing training for all employees on the threats posed by malware and the controls in place.

Network/System Analysts
The Network/System Analysts are responsible and accountable for:

- Verifying the endpoint security management console is being monitored to ensure that all computers and servers are using current application releases and appropriate security updates.
- Monitoring the endpoint security management console to ensure that all computers and servers are using current application releases and security updates.
- Coordinating with the Lead Technology Support Specialist to ensure the removal of malware when necessary.

Employees
Employees are responsible and accountable for:

- Monitoring individual workstations for malware and contacting the BUSD Technology Help Desk immediately if found. Employees shall not attempt to remove malware themselves.

4. MALICIOUS CODE GUIDELINES

BUSD's end security software will be installed on the following devices:

- PCs
- Macs
- Laptops
- Servers

Additional Guidelines

- Network/System Analysts will verify that updated malware signatures are downloaded to BUSD devices.
- Network/System Analysts will enable automatic scanning/real-time protection on all BUSD devices. End users cannot disable automatic scanning features.
- If malware is detected, the Technology Support Specialists will immediately isolate contaminated systems until the issue is resolved.
- The download and/or installation of unauthorized software is prohibited.
- Automatic scanning or real-time protection will be enabled in BUSD's standard endpoint security software for all devices. End users will not be permitted to disable these automatic scanning functions.
- All removable media (tapes, disks, USB drive, etc.) will be scanned for viruses/malware before using it in a BUSD computing device.
- A firewall will be implemented with the capability of eliminating as much malicious code (viruses, SPAM, etc.) as possible before ever entering BUSD's internal network.
- Only BUSD approved software will be installed on BUSD computers by Technology Support Specialists.
- The Network/System Analysts will provide a monthly security report to the Director of IT and Education Support documenting any malware activity and remediation.

Media Handling and Destruction Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to ensure that electronic- and paper-based media containing sensitive information is destroyed to reduce the risk that the information will be accessed and used by unauthorized individuals.

2. PURPOSE

These guidelines will document procedures for the proper disposal of electronic- and paper-based media containing sensitive information. Disposal procedures will depend on the type of media and the sensitivity of the information contained within. Media includes all paper documents and reports, microfilm, microfiche, magnetic tape, diskettes, CDs, other electronic media, or any other form of record containing sensitive information.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the Media Handling Guidelines.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Providing management oversight of BUSD's Media Handling and Destruction Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Ensuring that employees understand and adhere to media disposal and sanitation procedures to protect sensitive information.

Network/System Analysts and Technology Support Specialists
The Network/System Analysts and Technology Support Specialists are responsible and accountable for:

- Following NIST SP 800-88 Rev. 1 sanitization procedures on any electronic media that contains sensitive information and will be retired or reused for other purposes.

Employees
Employees are responsible and accountable for:

- Securely storing any electronic and paper media before leaving for the day.

4. MEDIA HANDLING AND DESTRUCTION GUIDELINES

The Director of IT and Education Support will ensure the media handling and destruction guidelines listed below are developed, implemented, and maintained to safeguard BUSD's sensitive information. The Director of IT and Education Support will instruct individual users periodically on their role and responsibilities relating to the handling of BUSD's electronic and paper media.

Paper Media

- Excluding permanent records, paper media containing sensitive information shall be shredded when the document is no longer needed and reaches the end of its retention period. Employees shall place paper media in a secured area prior to leaving for the day. No paper media containing sensitive information will be left overnight in unsecured trash cans.
- Employees shall not leave paper media containing sensitive information visible in their workspace when not physically present. Paper media containing sensitive information should be secured (i.e., locked desk drawer, locked office) prior to the user leaving their workspace.
- Employees working in areas accessible to the public shall secure paper media containing sensitive information from view.
- Employees shall store paper media in secure areas with limited employee and visitor access. BUSD has implemented the following controls to protect paper media:
    - Physical locks

Electronic Media

- When Electronic media containing sensitive information reaches the end of it's useful life, it shall be physically destroyed or sanitized according to NIST SP 800-88 Rev. 1.
- Employees shall not leave electronic media containing sensitive information visible in their workspace when not physically present. The electronic media shall be secured (i.e. locked desk drawer, locked office) prior to the employee leaving their workspace.
- Employees working in areas accessible to the public shall secure all electronic media.
- Employees shall store electronic media in secure areas with limited employee and visitor access. BUSD has implemented the following controls to protect electronic media:
    - Physical locks
- Employees are prohibited from downloading sensitive information onto any type or form of removable media unless expressly approved by the Director of IT and Education Support.
- If third-party providers (I.E. E-Waste, Device Buy-Back) are used to dispose of obsolete electronic equipment, each provider must certify that all electronic media was physical destroyed or sanitized according to NIST SP 800-88 Rev. 1.

Personnel Security Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to develop and maintain effective Personnel Security Guidelines, procedures, and controls to ensure the security of its information systems.

2. PURPOSE

The Personnel Security Guidelines will document required due diligence requirements for the hiring of new employees and contracting with third-party providers who will have access to sensitive information.

3. RESPONSIBILITY AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the Personnel Security Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Verifying that third-party providers are subject to screening procedures as required by the Vendor Management Guidelines.

Facilities and Technology Support (FTS)
The FTS is responsible and accountable for:

- Providing oversight of the Personnel Security Guidelines.

Human Resources
Human Resources is responsible and accountable for:

- Adhering to the due diligence requirements for the hiring of new employees.
- Verifying application information for new employees prior to hire.
- Completing criminal background and credit checks for all new employees prior to hire.
- Confirming the identity of new employees through the I-9 identification process.
- Determining when to require additional screening for sensitive positions.

4. PERSONNEL SECURITY GUIDELINES

The Board of Education shall establish the following guidelines to ensure the performance of proper due diligence when hiring new employees or contracting with third-party providers:

- Implementation of policies and procedures to mitigate risk posed by internal employees or external third-party providers who have access to and knowledge of BUSD's processes, systems, and data.
- Performance of criminal background and credit checks for all new employees.
- Confirmation of the identity of new employees according to the I-9 identification process.
- Verification that third-party providers are subject to similar screening procedures when necessary.
- Requiring additional screening procedures based on the sensitivity of the position, which may include:
    - Character references;
    - Confirmation of prior experience; and/or
    - Confirmation of academic or professional records.
- Requiring employees and third-party providers to sign confidentiality, nondisclosure, and acceptable use policies prior to granting access to system resources.
- Documentation and communication of relevant security roles and responsibilities for all employees within their job descriptions.
- Providing ongoing information security awareness and compliance training to all employees.

Physical Security Requirements Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to establish and maintain security controls to limit physical access to information systems and to protect the confidentiality, integrity, and availability of information.

2. PURPOSE

These guidelines establish the responsibilities for protecting physical information resources and sensitive information from threats including tampering, vandalism, or accidental damage.

3. RESPONSIBILITY AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the Physical Security Requirements Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Identifying, implementing, and enforcing physical security requirements for BUSD facilities to protect critical systems and sensitive information.
- Reviewing the effectiveness of physical security restrictions for all BUSD information systems components.
- Authorizing an employee to escort non-employees in restricted areas.

Director of Facilities
The Director of Facilities is responsible and accountable for:

- Identifying requirements for environmental protection of BUSD facilities.
- Authorizing an employee to escort non-employees in restricted areas.

School Principals

- Resetting access codes and collecting keys and door access cards after employee termination.
- Limiting building and restricted area access to those employees needing entry to fulfill job requirements.

Employees
Employees are responsible and accountable for:

- Securing all computers and related equipment in their possession.

- Reporting the loss or theft of information resources immediately to their direct supervisor.
- Remaining alert for non-employees (e.g., maintenance, customers, delivery personnel, third-party providers, etc.) and being prepared to challenge unfamiliar individuals entering restricted areas in BUSD.
- Keeping their work areas clean and storing sensitive information in secure locations when not in use.

4. PHYSICAL SECURITY REQUIREMENTS GUIDELINES

The following guidelines outline the steps BUSD will implement and maintain to restrict physical access or damage to its information systems.

- The Director of IT and Education Support will implement and maintain physical security controls to protect the confidentiality, integrity, and availability of information.
- The Director of IT and Education Support shall train employees on the proper procedures for securing equipment and sensitive information.
- The Director of IT and Education Support shall train employees on the proper procedures for handling visitors (i.e., vendors, etc.) who enter BUSD. Visitors will not be left unattended while in a restricted access area within BUSD. Employees will oversee all visitors while the visitor is in a restricted access area of BUSD.
- The following areas within BUSD require additional security measures and access shall be limited to authorized employees and contractors only:
    - Data Center
    - Technology Department Offices
    - Network Closets and Server Rooms
- Intrusion detection devices shall be installed and maintained to prevent theft and safeguard equipment. BUSD has installed the following intrusion detection devices:
    - Computer Labs
    - School Offices
    - District Service Center
    - District Office
- Environmental monitoring systems shall be installed and maintained to mitigate against the risks of fire and electrical outages. The devices installed include:
    - Fire Alarm
    - Fire Suppression Systems
    - Uninterruptible Power Supplies
- Physical security required for BUSD computer equipment shall be determined by the location of the equipment and the sensitivity of the data accessed. In unrestricted areas, automatic system timeouts shall be implemented. Whenever possible, employee computer screens shall not face public areas. The Director of IT and Education Support shall use employee awareness training and controls enforcement to ensure the effectiveness of security measures.
- Computer equipment will be protected by surge protection devices as appropriate to protect equipment from damage or loss of data.

- BUSD shall install Uninterruptible Power Supplies (UPS) to protect critical network devices (i.e. servers, switches, routers, firewalls) in the event of an electrical outage. The UPS shall provide battery power for sufficient time to allow the main office to continue making VoIP phone calls for at least one hour. A red power failure phone shall be provided in case of complete power loss.
- Computer rooms and other areas housing computer equipment will be kept at temperature and humidity levels recommended by equipment manufacturers. Temperature and humidity measurement devices will be installed in all computer rooms. The Director of IT and Education Support and the Technology Services Manager will oversee the monitoring of temperature and humidity levels in computer rooms.
- Computer wiring will be protected as appropriate by using conduit to encase wiring, avoiding routing wiring through publicly accessible areas, and avoiding routing wiring in close proximity to power cables.

Remote Access Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to develop and maintain effective Remote Access Guidelines procedures, and controls to ensure the security of its information systems. BUSD provides limited, controlled, and secure access to its LAN/WAN computing environment for authorized remote users.

2. PURPOSE

Remote access controls are required to ensure the integrity of information systems. Only authorized users and equipment will be allowed remote access connectivity.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the Remote Access Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Ensuring only authorized parties are allowed remote access to the network.
- Ensuring only approved equipment is used to access the network.
- Approving the third-party providers, contractors, and employees allowed to access BUSD's network remotely.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Oversight of the Remote Access Guidelines.
- Ensuring that remote access controls are implemented commensurate with the need and associated risks.

Network/System Analysts
The Network/System Analysts are responsible and accountable for:

- Monitoring, controlling, and logging remote access.
- Immediately revoking any remote access and securing any remote access devices of suspended or terminated parties.
- Maintaining a repository of approved VPN Access Request Forms.
- Performing a quarterly audit of VPN access.

Contractors
Contractors are responsible and accountable for:

- Completing and submitting a VPN Access Request Form at least one week prior to scheduled work.
- Obtaining prior approval to connect to BUSD's network.
- Ensuring the following requirements are met for all contractor systems used to remotely access BUSD's network:
    - Computer system is up-to-date with all security patches.
    - Automatic operating system updates are turned on.
    - Endpoint security software is installed and has the latest updates and signatures.
    - Endpoint security has performed a full scan of the computer in the last 7 days and active monitoring is enabled.

Employees

Employees are responsible and accountable for:

- Reviewing the Remote Access Guidelines and understanding its requirements.
- Notifying the Director of IT and Education Support if a third-party provider requires remote access to BUSD's network.
- Ensuring the following requirements are met for all personal employee systems used to remotely access BUSD's network:
    - Computer system is up-to-date with all security patches.
    - Automatic operating system updates are turned on.
    - Endpoint security software is installed and has the latest updates and signatures.
    - Endpoint security has performed a full scan of the computer in the last 7 days and active monitoring is enabled.

4. REMOTE ACCESS GUIDELINES

- The Director of IT and Education Support will ensure the remote access guidelines below are developed, implemented, and maintained to restrict remote access to BUSD's information systems to authorized users.
- The Network/System Analysts will configure third-party provider remote access upon the Director of IT and Education Support's approval and will monitor and terminate third-party remote access when the task is completed.
- Remote access to BUSD internal network will employ a secure remote access protocol to encrypt traffic and require user authentication to initiate a session.
- The Network/System Analysts will oversee the process of keeping all of BUSD's remote access hardware and software systems current with software patches and updates.

Security Awareness Training Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to establish a security awareness training program to enhance understanding of information security to reduce potential data loss due to user errors and omissions and to protect sensitive information.

2. PURPOSE

BUSD believes an educated and informed user base will contribute to the overall success of the Cybersecurity Guide. Therefore, the Director of IT and Education Support will ensure security awareness training sessions for all employees are conducted at least annually.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- Annually reviewing and approving the Security Awareness Training Guidelines.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Providing oversight of the Security Awareness Training Program
- Annually reviewing and approving the employee security awareness training schedule and attendance.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Leading the Facilities and Technology Subcommittee in the development, implementation, and maintenance of the Security Awareness Training Program.
- Ensuring that all employees participate in annual security awareness training.
- Maintaining the most recent version of the Guide policies on the network with shared access for all employees.
- The Security Awareness Training Program shall be available to staff by August 1st, 2020.

Assistant Superintendent, Human Resources
The Assistant Superintendent, Human Resources is responsible and accountable for:

- Ensuring that new employees review and affirm their understanding of the Guide by signing the Acceptable Use Agreement - Employee/Volunteer at hire.
- Verifying that a signed copy of the Acceptable Use Agreement - Employee/Volunteer form is stored in employee files.

Employees
Employees are responsible and accountable for:

- Reviewing and complying with the Guide policies.
- Signing and returning the Acceptable Use Agreement - Employee/Volunteer form to the Human Resources Department.
- Attending annual information security awareness training.

4. SECURITY AWARENESS TRAINING GUIDELINES

The Director of IT and Education Support will ensure the security awareness training guidelines below are developed, implemented, and maintained.

- The Director of IT and Education Support, or designee shall provide information security awareness training to all employees at least annually. They shall also maintain a record of attendees and training documentation. Training content shall include:
  - A review of all Cybersecurity Guide guidelines.
  - Procedures and best practices for protecting sensitive information.
  - New security threats.
- Each participant shall sign an acknowledgement of attendance and understanding of information security awareness training sessions.

Social Media Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to address the potential use of These guidelines have been developed to provide guidance to BUSD's employees and third-party providers on the risks of, and restrictions on, their use of social media for BUSD-related activities and for continued monitoring of BUSD's existing online presence.

2. PURPOSE

These guidelines establish BUSD's expectations use of social media channels and also guides BUSD's future social media planning and use. For purposes of these guidelines, social media includes all means of communicating information of any sort on the Internet, including on personal social media sites, blogs, newsgroups, and chat rooms.

3. RESPONSIBILITY AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- Annual review and approval of the Social Media Guidelines.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- Annual review of BUSD's Social Media Guidelines.
- Review and approval of BUSD's existing and future social media channels.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) is and is responsible and accountable for:

- Limiting employee access to social media sites from BUSD's internal network to only approved social media services.

Public Information Officer
The Public Information Officer is responsible and accountable for:

- Monitoring BUSD's social media presence, including comments or discussions posted regarding BUSD or its services, employees, and students.
- Responding to inappropriate, harassing, or abusive online communication regarding BUSD or its services, employees, and students.
- Future review and approval of employees authorized to develop BUSD's social media presence.

Employees

Employees are responsible and accountable for:

- Using good judgment to present themselves professionally both on and off duty.
- Refraining from participating in any social media activity during BUSD hours and on BUSD equipment unless authorized by the Director of IT and Education Support.
- Refraining from using BUSD email addresses to register for social media sites for personal use.
- Refraining from revealing or publicizing sensitive BUSD information including, but not limited to:
    - Financial information
    - Confidential student or district information
    - User account information
    - Internal email communication
- Refraining from posting or displaying comments about coworkers, supervisors, third-party affiliates, or BUSD that are vulgar, obscene, threatening, intimidating, harassing, or that could be perceived as abusive, hateful, demeaning, derogatory, or defamatory. This particularly includes any material causing or pertaining to unlawful discrimination, including discriminatory harassment, intimidation, and bullying, targeted at any employee or student by anyone, based on the employee or student's actual or perceived race, color, ancestry, nationality, national origin, immigration status, ethnic group identification, ethnicity, age, religion, marital status, pregnancy, parental status, physical or mental disability, sex, sexual orientation, gender, gender identity, gender expression, or genetic information, or association with a person or group with one or more of these actual or perceived characteristics.
- Notifying the Director of IT and Education Support of any inappropriate, harassing, or abusive online communication regarding BUSD or its services, employees, and students.

4. SOCIAL MEDIA GUIDELINES

The Director of IT and Education Support shall oversee BUSD's current and future online presence, including:

- Establishing appropriate firewall settings that restrict employee and student access to social media sites from BUSD's internal network.
- Maintaining overall awareness of social media trends and technologies.
- Addressing instances of the compromise of sensitive BUSD information via social media by activating the Incident Response Program (see Incident Response Program Guidelines).

If BUSD is mentioned in any social media activity, the posting must include the following disclaimer*: "The opinions expressed are my own and do not represent the opinion of Burbank Unified School District."* Only the Board of Education may speak on BUSD's behalf. Employees who violate any of the guidelines set forth in these guidelines may be subject to discipline, up to and including, termination of employment.

System Monitoring Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to establish appropriate protection of its network and sensitive information from unauthorized access and compromise by monitoring the security, performance, and integrity of its information systems.

2. PURPOSE

BUSD will ensure its systems are accessed only by authorized users, that only authorized changes are made to the systems, and that the systems perform as expected. The Network/System Analysts shall monitor BUSD systems and shall report all unauthorized attempts to access systems to the Director of IT and Education Support.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- The annual review and approval of the System Monitoring Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Review of the security exception reports.
- Providing training for all employees on the threats posed by malware and the controls in place.

Network/System Analysts
The Network/System Analysts are responsible and accountable for:

- Monitoring security logs to ensure systems are accessed only by authorized users.
- Review of the security exception reports.
- Maintaining a problem log of all outstanding issues related to critical systems, periodically reviewing logged issues, and monitoring trends in performance issues.
- Monitoring the appearance and content of the website for unauthorized changes or improper or unexpected applications of requested changes.
- Monitoring the network for the purpose of reporting and responding to significant discrepancies including:
  - Internal network usage
  - Security log
  - Application log

- System log
- Patch Management issues
- Remote control issues

- Maintaining a tracking report of all outstanding issues related to the network and providing the Director of IT and Education Support with a monthly network health report.
- Monitoring traffic on the firewall for the purpose of reporting and responding to significant discrepancies including:
  - Unauthorized access attempts
  - Intrusion attempts

Employees

Employees are responsible and accountable for:

- Monitoring individual workstations for malware and contacting the BUSD Technology Help Desk immediately if found. Employees shall not attempt to remove malware themselves.

4. SYSTEM MONITORING GUIDELINES

- The Director of IT and Education Support will ensure the system logging, review, and compliance guidelines listed below are developed, implemented and maintained to log, collect, and analyze data from system components. He will also establish and utilize standards to identify system components that warrant logging; determine the level of data to be logged by a component, and to establish guidelines for secure handling and analyzing of log files.
- Sufficient data will be collected in secure log files to identify and respond to security events and to monitor and enforce policy compliance.
- The following types of data will be monitored or logged to some extent:
  - Inbound and outbound Internet traffic
  - Internal network traffic
  - Firewall events
  - Virus/Malware events
  - SPAM events
  - Network and host performance
  - Application access
  - Remote network access
- The Network/System Analysts will monitor and restrict access to log files, which should not be overwritten and will be emailed in a monthly report to the Director of IT and Education Support.
- The Network/System Analysts will review system logs for suspicious activities on a daily basis and will report suspicious activities identified from log reviews to the Director of IT and Education Support, who will take action to resolve suspicious activity from log reviews as deemed appropriate.

Vendor Management Program Guidelines

1. INTRODUCTION

This policy has been developed to provide guidance on the information security controls for management of Burbank Unified School District's (BUSD) critical vendors. BUSD may contract with an outside vendor to service those products and services that require specific expertise or complex technology.

2. PURPOSE

These guidelines establish BUSD's expectations of and required controls for its third-party providers to ensure the security and integrity of our information systems and data. These guidelines also guide BUSD's ongoing third-party provider management and oversight responsibilities.

3. RESPONSIBILITY AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- Annual review and approval of the Vendor Management Program Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- The development, implementation, and monitoring of third-party provider management and oversight guidelines to ensure the risks and responsibilities of third-party relationships are clearly defined and maintained at acceptable levels.
- Annual reviews of BUSD's third-party providers and related FTS and Board reporting.

Facilities and Technology Subcommittee (FTS)
The FTS is responsible and accountable for:

- The implementation and maintenance of the Vendor Management Program Guidelines and related procedures.
- The review and approval of new third-party provider relationships.

4. VENDOR MANAGEMENT GUIDELINES

The FTS will ensure the vendor management and oversight guidelines listed below are developed, implemented, and maintained to ensure risks and responsibilities of third-party vendor relationships are clearly defined and maintained at acceptable levels.

- Due diligence and risk assessment requirements (see Exhibit 1 – Vendor Management Due Diligence Guidelines) for new third-party providers include, but are not limited to:

    - Financial statements;
    - Customer references;
    - Business continuity/disaster recovery plans and testing;
    - Information technology audit reports; and
    - Adequate insurance coverage.
- Specific contractual requirements including, but not limited to:
    - Contract term;
    - Termination requirements and penalties;
    - Service level requirements and reporting;
    - Adherence to regulatory requirements for safeguarding sensitive information, including requiring non-disclosure/confidentiality agreements;
    - Provision of periodic audit reports, including vulnerability and penetration tests and SSAE 18 SOC 2 Type II reports;
    - Incident response plan coordination and notification requirements;
    - Use of subcontractors; and
    - Ownership of BUSD data.
- The Director of IT and Education Support and the FTS shall review the services provided by each of BUSD's third-party providers to determine if it will be classified as a "critical" third-party provider. A critical third-party provider is an entity that provides services that must be continuously available to ensure information integrity, satisfactory service, and continuity and recovery of operations within a reasonable timeframe. Critical third-party providers include:
    - Cisco
    - Microsoft
    - Google
    - HP
    - Palo Alto
- The Director of IT and Education Support shall perform an annual review of BUSD's third-party providers and submit a summary report to the FTS.
- The Director of IT and Education Support shall use the Vendor Management Program Checklist (see Exhibit 2) when performing provider reviews. The checklist includes the following categories:
    - Financial condition;
    - Information system controls and audits;
    - Quality of service and support; and
    - Required documentation.

Wireless Networking Guidelines

1. INTRODUCTION

It is the policy of Burbank Unified School District (BUSD) to develop and maintain effective policies, procedures, and controls to ensure the security of its wireless networking services.

2. PURPOSE

The purpose of these guidelines is to describe how wireless networking is used in BUSD networks and the security controls protecting sensitive information.

3. RESPONSIBILITIES AND REPORTING

Board of Education
The Board of Education is responsible and accountable for:

- Annual review and approval of the Wireless Networking Guidelines.

Director of IT and Education Support
The Director of IT and Education Support serves as the Information Security Officer (ISO) and is responsible and accountable for:

- Approving the installation and configuration of wireless networking connected to BUSD networks.

Network/System Analysts
The Network/System Analysts are responsible and accountable for:

- Identifying appropriate methods of wireless networking and associated security controls within BUSD.
- Ensuring that the appropriate security controls are implemented.

Technical Support Specialists
The Technical Support Specialists are responsible and accountable for:

- Ensuring all wireless communication hardware is configured and updated appropriately.

4. WIRELESS NETWORKING GUIDELINES

The Director of IT and Education Support will ensure the wireless networking guidelines listed below are implemented and maintained to help safeguard BUSD's information systems.

1. District-owned devices will connect to the internal BUSD wireless network.
2. Guest users and BYOD devices will connect to the BUSD-Guest wireless network.

BUSD is implementing a network access control system.. Once completed, these guidelines should be followed:

1. District-owned and BYOD devices will connect to the internal BurbankUSD wireless network using their District username and password. If the device is a personal device it is required to pass a health/posture assessment before it is allowed onto the internal network. Here are the requirements:
    a. OS is up to date.
    b. Automatic updates are turned on.
    c. Endpoint security software is installed.
    d. Endpoint security software is up to date.

2. Guest users will connect to BurbankUSD-Guest wireless network. Visitors are required to request a temporary username/password assigned by an Office Manager/Administrative Secretary.

Exhibits

EXHIBIT 1

Vendor Management Due Diligence Guidelines

VENDOR SELECTION PHASE	
Type of Risk	Recommended BUSD Measures to Mitigate Risk
The vendor, due to financial weakness, could go out of business and, by doing so, significantly disrupt BUSD's services.	● Perform a financial analysis of vendor and determine whether or not to do business if there is significant financial weakness. ● At a minimum, consider having termination language in the contract to allow BUSD an "out" if such financial condition worsens. ● Create a contingency plan that allows for smooth conversion to an alternate provider in the event the provider does fail. ● Be sure to include all key vendors in this analysis.
The vendor's system may not meet BUSD's current and/or emerging needs, resulting in inefficient operations and services. Risk to BUSD's reputation can result accordingly.	● Develop a comprehensive Request for Proposal (RFP) or Decision Support matrix and compare several vendor offerings before making a selection. ● Consult with existing customers, user groups, and partners of the providers to gather information about the provider's reputation and performance. ● Consider engaging independent resources in supporting BUSD's evaluation process.
The vendor may lack appropriate operating or security controls, which, if breached, could cause financial or reputation loss to BUSD.	● Thoroughly review 3rd party reviews and/or complete SSAE 18 (Type I and II) reports to determine an appropriate level of controls exist. ● Review vendor contingency plans and the results of their completed tests. ● Ensure all locations that handle operations are included in scope of the review.

CONTRACT NEGOTIATION PHASE	
Type of Risk	Recommended BUSD Measures to Mitigate Risk
Ambiguity as to the scope of services to be provided and the corresponding responsibilities of the vendor and BUSD can cause delayed implementations, inefficient operations, and potential transaction losses.	● Ensure that the vendor's response to an RFP or other requests for written information is incorporated into the contract by reference. ● Request the vendor detail clearly the responsibilities of the vendor and BUSD during implementation and ongoing.
A standard contract provided by the vendor may protect the interests of the vendor with little or no protection for BUSD. BUSD risks exposure in the event of disputes that may arise from time to time during the course of the contract.	● Consider engaging outside counsel to customize contract and balance interests more equitably. ● Pay particular attention to the areas covering limitation of liability. Ensure the contract is explicit on the liability of the vendor in the event the security of their system is breached and financial loss results. ● Consider adding performance standards (i.e., system availability of 99+%) and penalties in the event the vendor fails to meet them. ● Carefully examine and negotiate the right to terminate the contract and penalties (if applicable).
The vendor's knowledge and observance of regulatory requirements applicable to its business, and those of BUSD is critical. The provider's failure to perform satisfactorily in this area can expose BUSD to potential criticism by its regulatory agency along with potential penalties.	● Ensure the responsibilities of the vendor and BUSD are clearly delineated in the contract. ● Ensure that the vendor's responsibility for security and confidentiality of BUSD's resources are specifically addressed. The provider's commitment to disclose security breaches to BUSD should be detailed in the contract.
The failure of the vendor to regularly share 3rd party audits, financials, and ongoing contingency plan testing can prevent BUSD from detecting potential problems with the vendor.	● Contract should detail the frequency with which these ongoing reports will be provided. ● Contract should stipulate that these reports will automatically be sent to BUSD.

IMPLEMENTATION PHASE	
Type of Risk	Recommended BUSD Measures to Mitigate Risk
The absence of sufficient human resources on the part of BUSD can delay the implementation, and ultimately hamper ongoing operations.	● Identify early on in the project the resources needed by BUSD, both in terms of time, expertise and experience. ● Ensure that appropriate resources are dedicated to the project from the beginning of the implementation to the system "cutover."
The absence of sufficient representation from different areas within BUSD can result in ineffective system setup, internal conflicts within the institution, and re-work during or after the system implementation.	● Establish from the outset a project "team" that provides sufficient representation of BUSD's key stakeholders. ● Establish project reporting from the team to senior management to ensure that decisions being made by the team are consistent with management strategy and direction. ● Develop a method by which to properly escalate when there is project slippage or conflict.
Absence of establishing adequate internal controls for new systems and/or processes can lead to operational losses and customer dissatisfaction.	● Request materials from the third-party provider and/or other BUSD's on new controls and processes they established when implementing the same system. Determine the appropriateness of such controls for BUSD. ● Clearly document new responsibilities of staff and include in job descriptions. ● Limit system access based on job need and establish appropriate segregation of duties and dual control procedures. Pay particular attention to risks in new system offerings.

ONGOING VENDOR OVERSIGHT	
Type of Risk	Recommended BUSD Measures to Mitigate Risk
The unexpected failure of a vendor can significantly disrupt BUSD and cause customer dissatisfaction. The ongoing financial pressures on the vendor could result in "softening" operating controls, which in turn could cause financial loss or dissatisfaction.	● Review ongoing financial information provided by the vendor. ● Continually review contingency plans and ensure that alternate providers remain viable options in the event primary provider fails. Ensure that cost and conversion timeframes are known and factored as part of ongoing plan. ● Review closely the updated contingency plan tests of the vendor and specific actions taken to address identified deficiencies. ● Follow up on deficiencies noted in audit reports and request written responses.
Failure of provider to perform service satisfactorily can cause disruptions to BUSD's operations.	● Assign responsibility within BUSD to monitor and evaluate the vendor on an ongoing basis. ● Ensure that service levels are being maintained, and that service outages are promptly reported and resolved. ● Document areas of dissatisfaction with vendor and maintain comprehensive records of the vendor's responses. ● Periodically meet with the vendor to review performance issues and assess the vendor's plans to improve. ● Take active role in vendor user groups and establish alliances to help oversee vendor performance, while sharing costs to do so.

ONGOING VENDOR OVERSIGHT (CONTINUED)	
Type of Risk	Recommended BUSD Measures to Mitigate Risk
Security breaches of the vendor's system or BUSD's system can cause losses.	● Continually review security policies, practices and reviews of the vendor's system. ● Have the internal audit function perform a review of both the controls the vendor employs as well as those of BUSD for adequacy and comprehensiveness. ● Determine the adequacy of preventative and detective controls for those transactions that involve funds transfers within or outside BUSD. ● Consider engaging 3rd party assistance in security intrusion testing in the event that such resources are unavailable within BUSD. ● Consider partnering with other BUSD's who use the same vendor in performing security reviews of third-party provider.
The vendor may not keep pace with customer requests for new products and/or services, potentially resulting in negative reputation, customer dissatisfaction and/or customer defection.	● Keep current with the vendor's product and service development plans for the coming year. ● Establish contact with other BUSD's who use the same vendor and determine their level of satisfaction with new product and service offerings.

EXHIBIT 2

Vendor Management Checklist

Financial Condition	Yes	No	N/A
Has there been an evaluation of the financial condition conducted at least annually and more frequently when risk is high or moderate and increasing?			
Was the analysis as comprehensive?			
Does BUSD have a copy of the vendor's audited financial statements?			
If applicable, are the vendor's financial obligations to subcontractors being met in a timely manner?			
Is the vendor's insurance coverage adequate?			
Comments:			

Controls	Yes	No	N/A
Has there been a review of audit reports (e.g. internal audits, external audits, SSAE 18 reviews, security reviews), as well as examination reports, if available?			
Does a current SSAE 18 Type I or II, or other audit review need to be obtained?			
Is there follow-up on any deficiencies noted?			
Does BUSD receive annual business continuance, disaster recovery, test results? If yes, is BUSD satisfied with these results?			
Do the vendor policies relating to internal controls and security ensure that they continue to meet BUSD's minimum guidelines and contract requirements?			
Is the vendor monitored to confirm that agreed-upon security measures, quality assurance reviews, and specified policies and procedures, are being implemented?			
Does BUSD utilize coordinated reviews with user groups, as applicable?			
Are business resumption restoration results acceptable to BUSD?			

If sensitive information is shared with the vendor, are applicable privacy notices and opt-out notices distributed to affected individuals?			
Does BUSD monitor changes in vendor personnel assigned to BUSD and their access rights, if any?			
Does the vendor use a layered anti-malware strategy (e.g. integrity checks, anomaly detection, system behavior monitoring, employee security awareness training, traditional signature-based anti-malware systems)?			
Does the vendor have controls in place to prevent potential insider threats (e.g. employee screening, dual controls, segregation of duties)?			
Are appropriate redundancy controls in place, and replicated backup data files segregated, to provide for sufficient recovery capabilities?			
Are specific procedures in place for the investigation and resolution of data corruption in response and recovery strategies?			
Does the vendor have appropriate security in place for virtualized cloud recovery services?			
Are plans and processes in place to reconstitute the vendor's operations after a destructive attack?			
Does the vendor utilize independent, redundant, alternative communications providers?			
Does the vendor have enhanced disaster recovery planning that includes the possibility of simultaneous attacks?			

Quality of Service and Support	Yes	No	N/A
Are service level agreements or service expectations clearly documented and agreed upon by BUSD and the vendor?			
Does BUSD regularly review reports and/or surveys documenting the performance relative to service-level agreements established?			
Are contractual terms and conditions being met?			
Are revisions to service-level agreements or other terms made when needed?			
Are performance problems documented and followed up on in a timely manner?			

Is the account executive or key vendor contact knowledgeable, responsive, and reliable?			
Does the vendor have the ability to support BUSD's strategic plan and goals?			
Is adequate training provided to BUSD employees regarding the products and/or applications provided by the vendor?			
Does BUSD provide a method for which their employees can voice complaints or concerns, and does BUSD review these and seek out a resolution?			
Are there scheduled meetings with the vendor to discuss performance and operational issues?			
Does the institution maintain documents and records regarding contract compliance, revision, and dispute resolution?			
Comments:			

Documentation	Yes	No	N/A
Is the vendor information, contacts, contracts dates, etc. maintained in a master third-party provider list?			
Is a valid contract current, centralized and securely maintained?			
Has there been a confidentiality agreement signed with the vendor that conforms to regulatory and legal requirements?			
Was an appropriate and documented planning process and due diligence performed when selecting this vendor?			
Does BUSD review regular risk management and performance reports received from the vendor (e.g. audit reports, security reviews, and reports indicating compliance with service-level agreements)?			
Does BUSD need to produce an annual written report to the Board, or a delegated committee, of the results of the ongoing oversight activities?			
Comments:			

EXHIBIT 3

Incident Response Notification Form

Description of Incident:

_____

_____

_____

Any information subject to unauthorized access: Yes or No

If Yes, What:

_____

_____

_____

_____

What action will be taken to protect affected individuals from further unauthorized access:

_____

_____

_____

_____

Phone number affected individuals can call for information or assistance:

_____

Reminder to affected individuals to stay vigilant over next twelve (12) to twenty-four (24) months and report suspected identity theft incidents to the institution.

_____