The Superintendent or designee will oversee the District's electronic communications system.

The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical use of this resource.

ISO 27001 OBJECTIVES AND CONTROLS

Technology services will follow industry standard ISO 27001, which specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system.

INFORMATION SECURITY POLICY

To provide management direction and support for information security in accordance with business requirements, relevant laws, and regulations:

1. An information security policy document will be approved by management and published and communicated to all employees and relevant external parties.
2. The information security policy will be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

INFORMATION CLASSIFICATION

To ensure that information receives an appropriate level of protection:

1. Information will be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.
2. An appropriate set of procedures for information labeling and handling will be developed and implemented in accordance with the classification scheme adopted by the organization.

CONSENT REQUIREMENTS

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the owner(s) or individual(s) the owner specifically authorizes may upload copyrighted material to the system.

No original work created by any District student or employee will be posted on a Web page under the District's control unless the District has received written consent from the student (and the student's parent) or the employee who created the work. [See CQ(EXHIBIT)]

No personally identifiable information about a District student will be posted on a Web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by

the Family Education Records Privacy Act (FERPA) and District policy. [See CQ(EXHIBIT) and policies at FL]

SYSTEM ACCESS

Access to the District's electronic communications system will be governed as follows:

1. District employees will be granted default access to the District's network, Intranet, Internet, Learning Management System (LMS), and e-mail system. Specific access will be granted as required to instructional and administrative applications, as well as shared folders and portfolios.

~~2. Students in kindergarten–grade 5 will be granted access to the District's system by their teachers, as appropriate. Students in grades 6–12 will be assigned individual accounts.~~

~~3. A teacher may apply for a class account and in doing so will be ultimately responsible for use of the account.~~

4. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system as identified above.

INTERNAL ORGANIZATION

To manage information security within the organization:

1. Management will actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

2. Information security activities will be coordinated by representatives from different parts of the organization with relevant roles and job functions.

3. All information security responsibilities will be clearly defined.

4. A management authorization process for new information processing facilities will be defined and implemented.

5. Requirements for confidentiality or nondisclosure agreements reflecting the organization's needs for the protection of information will be identified and regularly reviewed.

6. Appropriate contacts with relevant authorities will be maintained.

7. Appropriate contacts with special interest groups or other specialist security forums and professional associations will be maintained.

8. The organization's approach to managing information security and its implementation (i.e., control objectives, controls, poli-

cies, processes, and procedures for information security) will be reviewed independently at planned intervals or when significant changes to the security implementation occur.

TECHNOLOGY COORDINATOR RESPONSIBILITIES

The technology coordinator for the District's electronic communications system (or campus designee) will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.

2. ~~2.~~ Ensure that all users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file **VIA THE STUDENT ONLINE REGISTRATION SYSTEM OR EMPLOYEE HANDBOOK ACKNOWLEDGEMENTS.** ~~in the principal's or supervisor's office.~~

3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.

4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.

5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.

6. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.

7. Set limits for data storage within the District's system, as needed.

INDIVIDUAL USER RESPONSIBILITIES

ONLINE CONDUCT

The following standards will apply to all users of the District's electronic information/communications systems:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.

2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.

3. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.

4. Students may not distribute personal information about

themselves or others by means of the electronic communication system.

5. System users must purge and/or archive electronic mail to remain within allocated file size limits, in accordance with established retention guidelines.

6. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.

7. System users may upload public domain programs to the system. System users may also download public domain programs for their own use or may noncommercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.

8. System users may not send or post messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

9. System users may not purposefully access materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

10. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention. System users should therefore clarify the capacity in which they are sending or receiving electronic mail to prevent such misunderstanding from occurring.

11. System users may not waste District resources related to the electronic communications system.

12. System users may not gain unauthorized access to resources or information.

RESPONSIBILITY FOR ASSETS

To achieve and maintain appropriate protection of organizational assets:

1. All assets will be clearly identified and an inventory of all important assets drawn up and maintained.

2. All information and assets associated with information processing facilities will be "owned" by a designated part of the organization.

3. Rules for the acceptable use of information and assets associated with information processing facilities will be identified, documented, and implemented.

SECURITY RESPONSIBILITIES OF USERS

To prevent unauthorized user access, and compromise or theft of information and information processing facilities:

1. Users will be required to follow good security practices in the selection and use of passwords.
2. Users will ensure that unattended equipment has appropriate protection, primarily by locking workstations prior to leaving.
3. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities will be adopted.

HUMAN RESOURCES SECURITY (PRIOR TO EMPLOYMENT)

To ensure that employees, contractors, and third-party users understand their responsibilities and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud, or misuse of facilities:

1. Security roles and responsibilities of employees, contractors, and third-party users will be defined and documented in accordance with the organization's information security policy.
2. Background verification checks on all candidates for employment, contractors, and third-party users will be carried out in accordance with relevant laws and regulations and ethics, and will be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
3. As part of their contractual obligation, employees, contractors, and third-party users will agree to and sign the terms and conditions of their employment contract, which will state their and the organization's responsibilities for information security.

HUMAN RESOURCES SECURITY (DURING EMPLOYMENT)

To ensure that all employees, contractors, and third-party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error:

1. Management will require employees, contractors, and third-party users to apply security in accordance with established policies and procedures of the organization.
2. All employees of the organization and, where relevant, contractors and third-party users will receive appropriate aware-

ness training and regular updates in organizational policies and procedures, as relevant for their job function.

3. There will be a formal disciplinary process for employees who have committed a security breach.

TERMINATION OR CHANGE OF EMPLOYMENT

To ensure that employees, contractors, and third-party users exit an organization or change employment in an orderly manner:

1. Responsibilities for performing employment termination or change of employment will be clearly defined and assigned.
2. All employees, contractors, and third-party users will return all of the organization's assets in their possession upon termination of their employment, contract, or agreement.
3. The access rights of all employees, contractors, and third-party users to information and information processing facilities will be removed upon termination of their employment, contract, or agreement, or adjusted upon change.

EXTERNAL PARTIES

To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties:

1. The risks to the organization's information and information processing facilities from business processes involving external parties will be identified and appropriate controls implemented before granting access.
2. All identified security requirements will be addressed before giving customers access to the organization's information or assets.
3. Agreements with third parties involving accessing, processing, communicating, or managing the organization's information or information processing facilities, or adding products or services to information processing facilities will cover all relevant security requirements.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data or data of another user of the District's system or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with

system restoration, as well as other appropriate consequences. [See DH, FN, FO Series, and the Student Code of Conduct]

SECURE AREAS

To prevent unauthorized physical access, damage, and interference to the organization's premises and information:

1. Security perimeters (barriers such as walls, card-controlled entry gates, or manned reception desks) will be used to protect areas that contain information and information processing facilities.
2. Secure areas will be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
3. Physical security for offices, rooms, and facilities will be designed and applied.
4. Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster will be designed and applied.
5. Physical protection and guidelines for working in secure areas will be designed and applied.
6. Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises will be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

EQUIPMENT SECURITY

To prevent loss, damage, theft, or compromise of assets and interruption to the organization's activities:

1. Equipment will be sited or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.
2. Equipment will be protected from power failures and other disruptions caused by failures in supporting utilities.
3. Power and telecommunications cabling carrying data or supporting information services will be protected from interception or damage.
4. Equipment will be correctly maintained to ensure its continued availability and integrity.
5. Security will be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
6. All items of equipment containing storage media will be checked to ensure that any sensitive data and licensed soft-

ware has been removed or securely overwritten prior to disposal.

7. Equipment, information, or software will not be taken off-site without prior authorization.

PROTECTION AGAINST MALICIOUS AND MOBILE CODE

To protect the integrity of software and information:

1. Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures will be implemented.

2. Where the use of a mobile code is authorized, the configuration will ensure that the authorized mobile code operates according to a clearly defined security policy, and an unauthorized mobile code will be prevented from executing.

FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

INFORMATION CONTENT / THIRD-PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]

PARTICIPATION IN CHAT ROOMS AND NEWSGROUPS

Participation in chat rooms and newsgroups accessed on the Internet is permissible only for students in grades 9–12 (for assignments only), under supervision, and for employees.

DEVELOPMENT OF WEB PAGES

Procedures for development of Web pages are as follows:

1. The District will maintain a Web site and will develop Web pages presenting information about the District. The Chief

COMMUNICATIONS ~~Technology~~ Officer or ~~his or her~~ designee will act as Webmaster responsible for maintaining the District's Web site.

CAMPUS WEB PAGES

2. The District will provide templates for the campus Web pages as well as District-maintained information such as directories. The campus principal or the principal's designee will post material on and otherwise maintain content within, campus Web pages, including links to other sites. Material presented on the campus Web page must relate specifically to campus departments, organizations, or activities and will include only campus-produced material.

EXTRA-CURRICULAR ORGANIZATION WEB PAGES

3. With the approval of the campus principal, extracurricular organizations may establish Web pages. The principal will establish a process and criteria to establish and post material, including links to other sites, on these pages. Material presented on the organization Web page must relate specifically to organization and/or student activities. Organization Web pages must include the following notice:

> "This is a student extracurricular organization Web page. Opinions expressed on this page will not be attributed to the El Paso Independent School District."

[See FM(LEGAL)]

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is considered inappropriate.
4. Transmitting obscene messages or pictures is prohibited.
5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

OPERATIONAL PROCEDURES AND RESPONSIBILITIES

To ensure the correct and secure operation of information processing facilities:

1. Operating procedures will be documented, maintained, and made available to all users who need them.
2. Changes to information processing facilities and systems will be controlled.

3. Duties and areas of responsibility will be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

4. Development, test, and operational facilities will be separated to reduce the risks of unauthorized access or changes to the operational system.

THIRD-PARTY SERVICE DELIVERY MANAGEMENT

To implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements:

1. It will be ensured that the security controls, service definitions, and delivery levels included in the third-party service delivery agreement are implemented, operated, and maintained by the third party.

2. The services, reports, and records provided by the third party will be regularly monitored and reviewed, and audits will be carried out regularly.

3. Changes to the provision of services, including maintaining and improving existing information security policies, procedures, and controls, will be managed, taking account of the criticality of business systems and processes involved and reassessment of risks.

SYSTEM PLANNING AND ACCEPTANCE

To minimize the risk of systems failures:

1. The use of resources will be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

2. Acceptance criteria for new information systems, upgrades, and new versions will be established and suitable tests of the system(s) carried out during development and prior to acceptance.

TERMINATION / REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

PROTECTION AGAINST MALICIOUS AND MOBILE CODE

To protect the integrity of software and information:

1. Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures will be implemented.

2. Where the use of a mobile code is authorized, the configuration will ensure that the authorized mobile code operates according to a clearly defined security policy, and an unauthorized mobile code will be prevented from executing.

BACK-UP

To maintain the integrity and availability of information and information processing facilities:

1. Back-up copies of information and software will be taken and tested regularly in accordance with the agreed backup policy.
2. Users must routinely back up critical files on a District-shared drive **(ONEDRIVE)** ~~a commercial cloud drive (e.g., dropbox)~~, or on portable media (e.g., flash drives).

NETWORK SECURITY MANAGEMENT

To ensure the protection of information in networks and the protection of the supporting infrastructure:

1. Networks will be adequately managed and controlled in order to be protected from threats and to maintain security for the systems and applications using the network, including information in transit.
2. Security features, service levels, and management requirements of all network services will be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

MEDIA HANDLING

To prevent unauthorized disclosure, modification, removal, or destruction of assets, and interruption to business activities:

1. There will be procedures in place for the management of removable media, including locking such media in a secured location.
2. Media will be disposed of securely and safely when no longer required, using formal procedures.
3. Procedures for the handling and storage of information will be established to protect this information from unauthorized disclosure or misuse.
4. System documentation will be protected against unauthorized access.

EXCHANGE OF INFORMATION

To maintain the security of information and software exchanged within an organization and with any external entity:

1. Formal exchange policies, procedures, and controls will be in place to protect the exchange of information through the use of all types of communication facilities.

2. Agreements will be established for the exchange of information and software between the organization and external parties.
3. Media containing information will be protected against unauthorized access, misuse, or corruption during transportation beyond an organization's physical boundaries.
4. Information involved in electronic messaging will be appropriately protected.
5. Policies and procedures will be developed and implemented to protect information associated with the interconnection of business information systems.

ELECTRONIC COMMERCE SERVICES

To ensure the security of electronic commerce services and their secure use:

1. Information involved in electronic commerce passing over public networks will be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
2. Information involved in online transactions will be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay.
3. The integrity of information being made available on a publicly available system will be protected to prevent unauthorized modification.

MONITORING

To detect unauthorized information processing activities:

1. Audit logs recording user activities, exceptions, and information security events will be produced and kept for an agreed period to assist in future investigations and access control monitoring.
2. Procedures for monitoring use of information processing facilities will be established and the results of the monitoring activities reviewed regularly.
3. Logging facilities and log information will be protected against tampering and unauthorized access.
4. System administrator and system operator activities will be logged.
5. Faults will be logged, analyzed, and appropriate action taken.

6. The clocks of all relevant information processing systems within an organization or security domain will be synchronized with an agreed accurate time source.

BUSINESS REQUIREMENT FOR ACCESS CONTROL

To control access to information, an access control policy will be established, documented, and reviewed based on business and security requirements for access.

USER ACCESS MANAGEMENT

To ensure authorized user access and to prevent unauthorized access to information systems:

1. There will be a formal user registration and deregistration procedure in place for granting and revoking access to all information systems and services.
2. The allocation and use of privileges will be restricted and controlled.
3. The allocation of passwords will be controlled through a formal management process.
4. Management will review users' access rights at regular intervals using a formal process.

USER RESPONSIBILITIES

To prevent unauthorized user access and compromise or theft of information and information processing facilities:

1. Users will be required to follow good security practices in the selection and use of passwords.
2. Users will ensure that unattended equipment has appropriate protection, including locking screens when not in use.
3. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities will be adopted.

NETWORK ACCESS CONTROL

To prevent unauthorized access to networked services:

1. Users will only be provided with access to the services that they have been specifically authorized to use.
2. Appropriate authentication methods will be used to control access by remote users.
3. Automatic equipment identification will be considered as a means to authenticate connections from specific locations and equipment.
4. Physical and logical access to diagnostic and configuration ports will be controlled.

5. Groups of information services, users, and information systems will be segregated on networks.

6. For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network will be restricted, in line with the access control policy and requirements of the business applications [see business requirement for access control].

7. Routing controls will be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

OPERATING SYSTEM ACCESS CONTROL

To prevent unauthorized access to operating systems:

1. Access to operating systems will be controlled by a secure log-on procedure.

2. All users will have a unique identifier (user id) for their personal use only, and a suitable authentication technique will be chosen to substantiate the claimed identity of a user.

3. Systems for managing passwords will be interactive and will ensure quality passwords.

4. The use of utility programs that might be capable of overriding system and application controls will be restricted and tightly controlled.

5. Users must lock their workstations when they are away, and inactive sessions will shut down after a defined period of inactivity.

6. Restrictions on connection times will be used to provide additional security for high-risk applications.

APPLICATION AND INFORMATION ACCESS CONTROL

To prevent unauthorized access to information held in application systems:

1. Access to information and application system functions by users and support personnel will be restricted in accordance with the defined access control policy.

2. Sensitive systems will have a dedicated (isolated) computing environment.

MOBILE COMPUTING AND TELEWORKING

To ensure information security when using mobile computing and teleworking facilities:

1. A formal policy will be in place, and appropriate security measures will be adopted to protect against the risks of using mobile computing and communication facilities.

2. A policy, operational plans, and procedures will be developed and implemented for teleworking activities.

SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

To ensure that security is an integral part of information systems, statements of business requirements for new information systems or enhancements to existing information systems will specify the requirements for security controls.

CORRECT PROCESSING IN APPLICATIONS

To prevent errors, loss, unauthorized modification, or misuse of information in applications:

1. Data input to applications will be validated to ensure that this data is correct and appropriate.
2. Validation checks will be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
3. Requirements for ensuring authenticity and protecting message integrity in applications will be identified, and appropriate controls identified and implemented.
4. Data output from an application will be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

CRYPTOGRAPHIC CONTROLS

To protect the confidentiality, authenticity, or integrity of information by cryptographic means:

1. A policy on the use of cryptographic controls for protection of information will be developed and implemented.
2. Key management will be in place to support the organization's use of cryptographic techniques.

SECURITY OF SYSTEM FILES

To ensure the security of system files:

1. There will be procedures in place to control the installation of software on operational systems.
2. Test data will be selected carefully, protected, and controlled.
3. Access to program source codes will be restricted.

SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

To maintain the security of application system software and information:

1. The implementation of changes will be controlled by the use of formal change control procedures.
2. When operating systems are changed, business critical applications will be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

3. Modifications to software packages will be discouraged and limited to necessary changes, and all changes will be strictly controlled.
4. Opportunities for information leakage will be prevented.
5. Outsourced software development will be supervised and monitored by the organization.

TECHNICAL VULNERABILITY MANAGEMENT

To reduce risks resulting from exploitation of published technical vulnerabilities timely information about technical vulnerabilities of information systems being used will be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES

To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken:

1. Information security events will be reported through appropriate management channels as quickly as possible.
2. All employees, contractors, and third-party users of information systems and services will be required to note and report any observed or suspected security weaknesses in systems or services.

MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

To ensure a consistent and effective approach is applied to the management of information security incidents:

1. Management responsibilities and procedures will be established to ensure a quick, effective, and orderly response to information security incidents.
2. There will be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
3. Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence will be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption:

1. A managed process will be developed and maintained for business continuity throughout the organization that address-

es the information security requirements needed for the organization's business continuity.

2. Events that can cause interruptions to business processes will be identified, along with the probability and impact of such interruptions and their consequences for information security.

3. Plans will be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

4. A single framework of business continuity plans will be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

5. Business continuity plans will be tested and updated regularly to ensure that they are up to date and effective.

COMPLIANCE WITH LEGAL REQUIREMENTS

To avoid breaches of any law, statutory, regulatory, or contractual obligations, and of any security requirements:

1. All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements will be explicitly defined, documented, and kept up to date for each information system and the organization.

2. Appropriate procedures will be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect to which there may be intellectual property rights and on the use of proprietary software products.

3. Important records will be protected from loss, destruction, and falsification in accordance with statutory, regulatory, contractual, and business requirements.

4. Data protection and privacy will be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

5. Users will be deterred from using information processing facilities for unauthorized purposes.

6. Cryptographic controls will be used in compliance with all relevant agreements, laws, and regulations.

COMPLIANCE WITH SECURITY POLICIES AND STANDARDS AND TECHNICAL COMPLIANCE

To ensure compliance of systems with organizational security policies and standards:

1. Managers will ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

2. Information systems will be regularly checked for compliance with security implementation standards.

INFORMATION SYSTEMS AUDIT CONSIDERATIONS

To maximize the effectiveness of and to minimize interference to/from the information systems audit process:

1. Audit requirements and activities involving checks on operational systems will be carefully planned and agreed to minimize the risk of disruptions to business processes.

2. Access to information systems audit tools will be protected to prevent any possible misuse or compromise.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on, the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.