| TOPEKA PUBLIC SCHOOLS | REGULATION NUMBER: 2935-2 |
|---|---|
| SUBJECT:<br><br>COMPUTER AND ELECTRONIC SECURITY RESPONSIBILITIES AND PROCEDURES | DATE OF ISSUE: 07/06/07<br>REVISIONS: 12/03/09; 06/18/10; 06/03/11<br>PREPARING OFFICE: ADMINISTRATIVE AND SUPPORT SERVICES |

## I. BACKGROUND:

**The need for computer and electronic security is established by Topeka Public Schools' policies approved by the Board of Education for Topeka Public Schools USD 501 (hereinafter referred to as TPS). Any TPS staff member who requires access to various computer systems and applications in order to enter, update, and produce reports containing school-related information/data may apply for this access. Various TPS, state and federal entities as well as students and parents use this information. The dissemination of much of this information is subject to state and federal laws and TPS policies and regulations. Therefore, it is the responsibility of TPS to safeguard not only the physical access to computers and the information contained in the TPS computer systems, but to provide for the electronic security of all computer systems and information.**

## II. PURPOSE:

**The purpose of this regulation is to define procedures to be followed to safeguard access to the computer systems, data applications, and electronic information available through these systems. These procedures ensure that only authorized persons are able to enter, update and manage data for the areas that they are responsible. These procedures are also designed to preclude access to systems, applications and information by TPS staff, students, parents, and non-employees outside of their designated responsibility.**

## III. PERSONNEL AFFECTED:

**Any individual who has been granted access to TPS technology systems is required to follow the procedures outlined in this regulation.**

**Definitions:**

**<u>Password</u> – is a set of characters and/or numbers which, along with the user ID, is a person's key to access the Topeka Public Schools data network and computer applications.**

**<u>User ID</u> – is a name used to identify the user when signing on to the Topeka Public Schools data network and computer applications.**

**Center Manager/School Principal – The center manager/school principal is a TPS administrator who has been given the responsibility to manage a TPS building, department, or program by the Superintendent and/or the Board of Education.**

**Computer and Electronic Security – In general, computer and electronic system security is the capability to control and manage physical access to the computer or electronic equipment, electronic access to the equipment and applications, and user access to electronic data and applications.**

**Network – The communications medium that provides connectivity between TPS's computer systems, enables the use of TPS electronic information applications, and provides for the storage and retrieval of electronic data. The network connects all TPS buildings via fiber optic, copper wiring systems, network switches and routers.**

**Network Security – Network security is the processes and procedures that either provides access to authorized persons, or denies access to unauthorized persons to the network, applications and electronic information. Network security also limits authorized users' access to only those applications and information required to fulfill their responsibilities. Each authorized user is provided a TPS assigned login name and user selected password to access network resources, applications and information.**

**Network Account – A network account provides staff, students, and selected individuals with secure access to the TPS network, applications and electronic information. The access provided is determined by their specific position, assignment, responsibilities and facility. Individual network accounts are protected by the network security described above. User's responsibilities for network accounts are described in other TPS policies and regulations.**

**AS/400 – The AS/400 will designate both the computer hardware platform and the operating system that runs the TPS mission critical (TERMS) applications. The AS/400 is located at the Information Technology Department in the Lucinda Todd Education Center building.**

**AS/400 Security – Access to the TERMS application is controlled by the security access granted to the user in the AS/400 security system. Users who have been granted AS/400 access security rights to applications are required to belong to a specific group in the TPS.**

**TERMS – This is an acronym meaning Total Educational Resources Management System. TERMS, for purposes of this document, consists of five integrated modules that allow data to be entered, stored, and shared between modules and reports. The five modules are Administration, Financial, Human Resource, Warehouse, and Student Information. There are sub-modules within each system that address specific sub-tasks for each main module. The TERMS application is located on the district's AS/400 computer system.**

**TERMS Security – Included in the TERMS Administration module is the capability to assign access rights to TPS users for the various modules and screens. Within the modules and screens, access rights may be given for update or view only rights to each screen and module report. While access to the TERMS application is controlled by the AS/400 security system, the TERMS administrative module and the access rights assigned to each user controls access to the various modules within TERMS.**

**TERMS Profile – A TERMS Profile groups together Job Title Codes, responsibility centers, and Job Title Descriptions that are similar in nature and require the same basic TERMS authorizations. These groups generally have the same information and functionality to successfully perform TPS functions. TERMS Profiles are assigned for business functions, (finance, human resource, and warehouse). Each TERMS Profile is further broken down by specific panels/screens available through the specified profile and the level of access assigned for each panel. Attachments 1 and 2 of this regulation identify the various profiles and the jobs associated with each profile. TERMS security is initially based on the assignment of TERMS access rights pertaining to an individuals' Job Title Code, responsibility center, and building assignment. The initial TERMS account assignment is based on these elements, as entered by the Human Resources Department during job assignment. The TERMS user groups for finance/budget/warehouse, human resources/payroll, and Information Technology authorize changes to these profiles. Since buildings may internally assign various responsibilities to different positions, the Center/Building Manager may submit change requests for individual TERMS user accounts. Information Technology profiles are not assigned by Job Title Code, but rather by job responsibility.**

**PowerSchool – Topeka Public Schools switched to PowerSchool as their Student Information System effective July 1, 2010.**

**PowerSchool Security – Included in the PowerSchool Administrative Group is the capability to assign access rights to TPS users for the various groups and panels/screens. Within the groups and screens, access rights may be given for update or view only rights to each panel/screen.**

**PowerSchool Groups – A PowerSchool Group is assigned by the employees Job Title Code, and is given access based on their responsibility center(s). Attachment 1 of this regulation identifies the various groups and jobs associated with each one. The initial PowerSchool account assignment is based on the information entered by the Human Resources Department during job assignment and the Center Manager/School Principal request. Many buildings internally assign various responsibilities to different positions; the center/manager may submit change requests for individual PowerSchool user accounts. Information Technology groups are assigned by job responsibility.**

**Job Title Code – The Job Title Code is a four-digit code associated with a specific job description. The Job Title Code is used to designate employees performing the same or similar functions within TPS. Each employee is further assigned a Position Code**

**composed of the nine digits (four-digit Responsibility Center where the employee is assigned, a single letter Group Code indicating the employee classification, and the four-digit Job Title Code). The Human Resources Department is responsible for assigning the correct Job Title Code/Job Description and Position Code for each employee. The Job Title Code is used to determine access to district technology and electronic information. Human Resources will create a new Job Title Code/Job Description as needed. Information Technology, working with the appropriate approval authority will create a new TERMS default profile to be assigned to the new Job Title Code/Job Description and assign the new job title code/job description to PowerSchool, This process insures that the employee receives the TERMS access required by the new position and is approved by the appropriate approval authority.**

**New Job Title Code - When a new Job Title Code/Job Description has been assigned or there has been a change in responsibilities for an employee the request must be in writing and approved by the appropriate Executive Director. The TERMS Profile Group to be assigned to the new Job Title Code/Job Description must be included in the request. Information Technology will be provided with the approval and a copy of the new Job Title Code/Job Description to determine the appropriate TERMS Profile. This process insures that the employee receives the TERMS access required by the new position and is approved by the appropriate executive director.**

**Portal Services Account – A portal service account provides access to TPS information/data associated specifically with the individual owning the account. Portal accounts are accessed through Internet or intranet services using an Internet browser. The security on the users' existing network, AS/400, TERMS and/or PowerSchool accounts determine the applications and information available through the portal services account.**

## IV. DISCUSSION:

**There are four broad classifications of TPS network users: employees, students, parents and non-employees.**

1. **Employees: Persons hired by TPS on a full or part time basis to perform a specified function within TPS and who receive TPS employee benefits are considered employees.**
2. **Students: The student classification includes full or part time persons who are taking instructional courses offered by the TPS as part of its normal curriculum with the course of study leading to a high school diploma.**
3. **Parents: Parents of TPS students are provided limited, secure access to information concerning their student(s).**
4. **Non-Employees: Non-employees include a variety of persons associated with TPS who require access to specific TPS technology resources or information. This classification may include employees who do not receive TPS benefits, but require access to TPS technology systems and information.**

**Network users will initially be assigned a network account with the network security described above in accordance with the procedures in this regulation. Based on the user's**

**job title code and building assignment and responsibility center, employees and non-employees may further be assigned a TERMS and/or PowerSchool account, subject to the TERMS and/or PowerSchool security authorization policies. The TERMS account will provide access to financial, human resource, or warehouse information that is necessary for the user to perform the functions required by their position. The PowerSchool account will provide access to the student information system based on the non-employees center and Job Title Code set up by Human Resources. In a very limited number of cases, employee access to the TERMS administrative module will be provided as part of the employees' TERMS account. There are only a few employees who will have access to the PowerSchool administrative account.**

**Access to the programming code for TERMS and/or PowerSchool and other AS/400 based applications is limited to specific personnel in TPS' Information Technology Department (ITD). Direct access to the AS/400 security application, utilities and operating system is also limited to specific personnel in the Information Technology Department. ITD personnel with access to TERMS and/or PowerSchool and AS/400 applications code will not have access to the AS/400 security module, utilities and operating system and vice versa.**

## V. PROCEDURES:

**The following describes the process of assigning security access for network resources, TERMS/PowerSchool, and the procedures to expand or restrict access for an individual based on the general classification of the individual and their assigned functions.**

**A. Employees are provided a basic, secure network account through an automated process based on their pay type and building assignment/responsibility center. The information entered by the Human Resources Department concerning an employee's pay type, job function(s), and building-assignment determine the extent of their network access and applications automatically assigned to the employee. Included in the network account are: a personal data storage area on the network (P:\ drive), a shared network storage area (S:\ drive), an e-mail account, Internet access, the TPS standard productivity suite, and, instructional and reference applications. The network account also provides off-site access through the TPS portal services to the employee's TPS e-mail and network storage areas. This allows access to site-specific applications based on their pay type, building- assignment, job function, or extra assignments as specified by the building/center manager. A new employee will be notified of the creation of their new network account through the building Technical Assistant to which they are assigned.**

**B. Access to a network account and subsequently to all other TPS technology accounts will be disabled automatically (within 24 hours of their departure) whenever an employee resigns or is terminated. Accounts will not be disabled for employees who are on short-term leave, such as vacation or FMLA. Employees taking a long-term leave of absence will have their accounts disabled. When an account is disabled, it will not be available to the user. The stored data of the resigned or terminated employee will remain intact for a period of ninety (90) days during which time the data (e-mail,**

**P drive) may be provided to other employees as directed by the building/center manager.**

**C. Employees will be automatically assigned access to TPS' TERMS and PowerSchool applications based on their job title and responsibility center assignment. These assignments are based on profiles established for the TERMS (Financial/Personnel systems access, Fiscal Services Department Human Resources Department and Groups for student system, PowerSchool). These profiles are listed in Attachment (1). The automated Default Job Title profiles are provided in Attachment (2). Attachments (3), (4), (5), (6), (7), and (8) provide a listing of the individual TERMS and/or PowerSchool profile descriptions.**

**Employees who are granted TERMS access will have one active TERMS session. Should an employee need to log on to TERMS multiple times, Request for Multiple TERMS Sessions (Attachment 12) should be signed by the appropriate center/facility manager, and forwarded to the General Director of Information Technology for approval.**

**D. Portal services accounts are provided as part of the network account. A person employed as a substitute TPS staff member will be provided with a portal account that provides access only to the Smart Find Express for the purpose of obtaining work assignments. Employees must have a separate Parent PowerSchool Account (discussed later) if they have students attending Topeka Public Schools.**

**E. This regulation, including all attachments and default profiles, will be reviewed annually. The attachments of this regulation will be revised independently. All attachment revisions will be approved by the superintendent or a designee of the superintendent. Default profiles will be reset based upon recommendation from the external auditing firm.**

**F. In the event that an employee requires authority to update or access TERMS information not available through the screens assigned by their default profile, building principal/center managers may request access to the information as an exception for the individual employee. To authorize the required access, their building principal/center manager must follow these procedures:**

**1. Determine that the building principal/center manager has been given authorization to access or the responsibility to maintain the desired information. The building principal/center manager cannot pass access rights or responsibilities that have not been provided to the building/center.**

**2. Determine exactly the information that is needed by the employee, the access rights required, and the miscellaneous profile(s) or screen(s) that contain the information. Attachment (9) lists the available screens. With this information established, the TERMS Authorization Change Form (Employees, Attachment [11]) – requests will not be accepted by e-mail or by telephone) shall be completed, including the signature of the building/center manager on the dated form, and**

**sent to Information Technology for review.**

3. **Upon receipt in Information Technology, the completed TERMS Authorization Form (Attachment [11]), will be date-stamped, photocopied and filed for tracking and status checking. The initial review of the completed form by the User Support Specialist (Help Desk) staff will occur within two business days of receipt. The review will be in several broad areas. These areas are as follows:**

    a. **Errors & Omissions – this review may result in adjustments to changes being made to the original submitted form. All adjustments to changes will be communicated and copies provided to the originating facility/center manager.**

    b. **Global changes – this review will be to assess if the requested change should be included in the automated process based on pay type, job function, job titles, and center assignments.**

    c. **The center manager/school principal will complete the appropriate change form (attachment 11) for the employees in their building of responsibility. They will forward these change forms to Information Technology for staff review. The staff will then forward to the appropriate director, general director, or executive director for their approval, signature and date.**

    d. **Upon receipt of the change form, the approval authority will have five business days to approve or deny the changes presented. In the event that the form is not received in the Information Technology department by the end of the sixth business day, the Information Technology staff member will then electronically forward a copy of the proposed change form to the supervisor of the approval authority for approval.**

    e. **Approved or denied, the security authorization forms will be returned to Information Technology where the Help Desk will perform a final review of said document, act on approvals granted, and notify interested parties. The final copy of the TERMS and/or PowerSchool authorization will be filed in the Information Technology department for safekeeping.**

4. **In the event that a request is disapproved, an appeal may be made to the Executive Director of Operations.**

G. **Authorizations for an employee to have access rights to specialized networked resources and applications are controlled and authorized by the building/center manager of the division, department, entity or program with responsibility for managing the resource or application. (Example: the General Director of Food and Nutrition Services must authorize access to all TPS food services applications.) All approved requests for access to these specialty systems must be forwarded in writing, using attachment 10, (Request for TPS Network Account and Applications form) to**

**Information Technology by the Building/Center Manager authorizing the changes.**

**On occasion it becomes necessary to review the electronic contents of an employee's network or local electronic resources. Facility/center managers will make all such requests to the TPS school district attorney who will obtain permission for the review from the superintendent or designated representative. The TPS school district attorney will notify the General Director of Information Technology in writing that a review of the employee's electronic resources has been approved. Upon completion of the review, the General Director of Information Technology will provide a written report to the TPS school district attorney and the school principal/center manager initiating the request.**

## VI. STUDENTS:

**Students are provided a basic, secure network account through an automated process based on their student status and attendance center. Included in the network account is a personal data storage area on the network (P:\ drive), a shared network storage area (S:\ drive), an e-mail account, Internet access, the TPS standard productivity suite, and TPS instructional and reference applications. The network account will also provide the student access to building/center specific applications based on the building the student is enrolled in. Access to applications required by enrollment in specific courses using computer labs and available only in those computer labs will be controlled by the course instructor. The student will be notified of their new network account through the attendance building.**

**Student network accounts will be transferred from one TPS building to another based on the information entered in the TPS's student information system concerning transfer dates. Access to network accounts and subsequently to all other TPS technology accounts for students will be deleted automatically whenever a student leaves the district. The process is automated similar to employee account management.**

**Students will not be provided direct access to the AS/400 or any application that operates on the AS/400 platforms. This prohibition includes TERMS and/or PowerSchool and all applications associated with the TERMS and/or PowerSchool system.**

## VII. PARENTS:

**Parents of Topeka Public Schools USD 501 students are offered a secure Internet connection to access information about their student(s). The Parent PowerSchool Account may provide student information, including grades and attendance, grade history, current schedules, allow e-mail notifications, e-mail teachers, class registration and class calendars. Information provided reflects data as it becomes available. This account is not a network or TERMS account and cannot be used to access the district network or TERMS system.**

**The parent PowerSchool account is accessed using the Internet through a secure network account issued by the district (Parent PowerSchool Account). Access to the Parent**

**PowerSchool is through the Topeka Public Schools' Web site, www.topekapublicschools.net A USERID and PASSWORD will be required to access student information. Parents may apply for a Parent PowerSchool Account at the school(s) attended by their student(s) using Application for Parent PowerSchool (Attachment 14).**

**In addition to information provided to TPS as part of the Pupil Information Form (PIF) used for student enrollment, for security reasons parents will be asked to provide photo identification such as a driver's license or military ID that contains a unique identification number for assigning parents an account. The use of this unique identification number allows TPS to provide a single USERID and PASSWORD to a parent to access their students at different schools using a different login account for each student.**

**In order for a parent to access information on their child, the parent's demographic information must appear on the student access list in the student's demographic information. The unique parent ID can only be validated at the school(s) that the student(s) attends.**

**When a student becomes 18 years old, the student's information cannot be provided to the parents without the specific permission of the student. Parents will be notified in advance of their student turning 18 so that they may discuss this issue with the student. If the student agrees to the parent accessing the student's information, the student must complete and sign a separate form, Student Permission for Parent PowerSchool Access (Attachment 15), specifically granting Parent PowerSchool access to designated individuals. As necessary, a letter is printed and sent out to the parent for students who will be turning 18.**

**When the parents/guardians have completed the necessary application for Parent PowerSchool Account, a letter is generated to the parent/guardian concerning the status of their Parent PowerSchool Account. The letter will provide TPS assigned USERID, a temporary PASSWORD and instructions for initially accessing their Parent PowerSchool Account and creating their own PASSWORD. This allows the parent access to student information for the student(s) associated with the Parent ID number provided on the Parent PowerSchool application.**

**The Parent PowerSchool Account is limited to information concerning a parent/ guardian's student(s). TPS employees with students attending district schools will be required to apply for and receive a separate Parent PowerSchool Account to access their student's information. This access is not included in an employee network account.**

## VIII. NON-EMPLOYEES:

**All persons or groups not described above as an employee, student, or parent/guardian are considered non-employees. There is no automated or default process to assign network accounts, TERMS and/or PowerSchool accounts, or AS/400 accounts. Each person in the non-employee classification will be individually assigned accounts based only on the requirements for secure access to the TPS' network, applications and information**

**as determined by the TPS.**

**Facility/center managers are responsible for confirming a non-employee's requirements for access, applying for the specific access rights required, and supervising the non-employee's use of the secure accounts provided. Attachment 10, Request for TPS Network Account & Applications form, must be used to request a TPS network account and access to controlled applications. E-mail and telephone calls will not be accepted. Applications for network accounts will be made to the General Director of Information Technology. To obtain access to TERMS and/or PowerSchool information, non-employees will follow the procedure as outlined above for TPS employees. All information must be entered on the Terms and/or PowerSchool Authorization forms, signed and dated. In no circumstances will non-employee accounts be issued for a period longer than 365 calendar days. Non-employee accounts to the network and TERMS and/or PowerSchool information must be renewed at least annually.**

## IX. ATTACHMENTS:

**The following attachments are listed for your reference:**

**(1) TERMS/PowerSchool Profiles**
**(2) Default Job Title Profiles by Job Title**
**(3) Student Profile descriptions**
**(4) Financial/Personnel Profile descriptions**
**(5) Fiscal Service Profile descriptions**
**(6) Human Resource Profile descriptions**
**(7) Facilities/Warehouse Profile descriptions**
**(8) Information Technology Profiles descriptions**
**(9) TERMS/PowerSchool Panels – All Administrative, Financial, Human Resources, Facilities/Warehouse and Student**
**(10) Request for District Network Account and Applications**
**(11) TERMS Authorization Form – Employee**
**(12) Request for Multiple TERMS Sessions Form**
**(13) PowerSchool Authorization Form**
**(14) Application for Parent PowerSchool Account**
**(15) Student Permission for Parent PowerSchool Access**