Title: User and Administrative Account Access		Code Number: IT.003.05
Functional Category: Information Technology Services	Issuing Department: Information Technology Services	Effective Date: 10/01/2018

1.0 PURPOSE

1.1 To establish policy to grant, modify, and remove access to the Board's electronic communication systems; to limit authorized rights and privileges to the minimum required to effectively fulfill the user's or system administrator's responsibilities; and to otherwise define types of accounts.

2.0 DEPARTMENTS / PERSONS AFFECTED

2.1 All employees, consultants/contractors, and any other authorized users of the Board's electronic communication systems.

3.0 POLICY

3.1 **Separation of Duties**.

3.1.1 Appropriate separation of duties must be maintained between development, test, and production environments. Developers must not have update access to production data.

3.1.2 Separation of duties applies to all account types specified in this policy.

3.2 **Cardholder Data Access Controls.**

3.2.1 Access to the Board's system components that store, process, and/or transmit credit card data must be limited to only those individuals whose jobs require such access as follows:

3.2.1.1 Access rights for privileged user IDs must be restricted to least privileges necessary to perform job responsibilities.

3.2.1.2 Approval by the Vice President of Information Technology Services (ITS) or the Assistant Vice President of Technology Security must be submitted in writing (or electronically) specifying required privileges

3.3 **User Accounts.**

3.3.1 Only users with documented authorization may access the Board's electronic communication systems.

3.3.2 Authorized users of the Board's electronic communication systems will be limited to "least privilege."

3.3.3 Authorized users requiring access to departmental restricted secure drive (data files) must obtain approval from the respective data owner by submitting the online Change Network Access Request form via Connected Online.

3.3.4 Only users with documented authorization may be granted Administrative Authority on their assigned workstation. Users with administrative authority on their assigned workstation must comply with all Board policies and the following activities are strictly prohibited:

3.3.4.1 Installing any non-standard or unlicensed software without concurrence from Information Technology Services (ITS).

3.3.4.2 Modifying any user or user group without authorization from ITS.

3.3.4.3 Circumventing any operational or security controls.

3.3.5 Local administrative authority may be revoked at any time by ITS without prior notice.

3.3.6 Authorized users will be issued individual user accounts with a unique user ID and password to be used in accessing the Board's electronic communication systems.

3.3.7 User accounts will expire or be disabled as follows:

3.3.7.1 **Regular Full-Time, Contract Full-Time, and Temporary Employees.** Effective date of resignation/involuntary termination, date the user account is no longer needed for the user to perform his/her Board duties, or upon authorization from:

3.3.7.1.1 The Vice President of ITS or the Executive Vice President of Administration and Diversity in the event of security concerns; or

3.3.7.1.2 The Executive Vice President of Administration and Diversity or the Vice President of Human Resources in the event of potential corrective action, an active investigation, or other HR related issue.

3.3.7.2 **Board Members.** At the completion of service on the Board.

3.3.7.3 **Consultants/Contractors.** Six months from creation date or completion of the assignment, whichever is less.

3.3.8 User accounts must have documented authorization to be re-enabled or extended.

3.3.9 User accounts are subject to review and audit.

3.3.10 Access to another user's electronically stored or transmitted information must comply with the Electronic Communication Systems Usage policy.

3.4 **System Administrator Accounts.**

3.4.1 Only users with documented proper justification and documented authorization from the Vice President of ITS or any assistant vice president of ITS will be granted system administrator accounts to the Board's electronic communication systems.

3.4.2 Authorized users with system administrator accounts will be limited to "least privilege."

3.4.3 Authorized users with system administrator accounts will use unique individual user IDs and passwords to access the Board's electronic communication systems.

3.4.4 System administrator accounts will expire or be disabled as follows:

3.4.4.1 **Regular Full-Time, Contract Full-Time, and Temporary Employees.** Date of resignation/involuntary termination, date the user account is no longer needed for the user to perform his/her Board duties, or upon authorization from:

3.4.4.1.1 The Vice President of ITS or the Executive Vice President of Administration and Diversity in the event of security concerns; or

3.4.4.1.2 The Executive Vice President of Administration and Diversity or the Vice President of HR in the event of potential corrective action, an active investigation, or other HR related issue.

3.4.4.2 **Consultants/Contractors.** Six months from creation date or completion of the assignment, whichever is less.

3.4.5 System administrator accounts must have documented authorization to be re-enabled or extended.

3.4.6 System administrator accounts are subject to review and audit.

3.4.7 Access to another user's electronically stored or transmitted information must be in compliance with the Electronic Communication Systems Usage policy.

3.5 **System Accounts.**

3.5.1 System accounts can be created and used to access Board electronic communication systems only upon presentation of documented need, the name of the system or software for which it is to be used, and documented authorization by the Vice President of ITS.

3.5.2 Authorized system accounts require the use of a unique system ID and password to access the Board's electronic communication systems.

3.5.3 System account passwords do not expire (for example, system accounts used to access backup systems).

3.5.4 System accounts will be disabled in order to maintain security and deleted after 180 days of no activity.

3.5.5 System accounts are subject to review and audit.

3.5.6 System accounts shall only be used to access the network for their intended purposes, and not be used for access in lieu of unique user accounts. All system accounts shall be properly documented in the "properties tab" of the account with applicable application/software name.

3.6 **Root Account.** Direct access to the root account is prohibited. System administrators and database administrators must first log in with an individual account and then be switched to the root account to establish individual accountability for their actions.

3.7 **Default Accounts.**

3.7.1 Passwords on all default accounts created through the installation of software, operating systems, and firmware for networks, devices, databases, and applications shall be changed to unique passwords upon installation to avoid the possibility of unauthorized access to Board systems.

3.8 **Device Accounts.**

3.8.1 Device accounts may be requested from the Vice President of ITS to enable access by a device where a clear, ongoing need for their use can be defined. Examples include accounts for kiosks, training computers, and computers used in DPS vehicles.

3.8.2 Device accounts require a unique system ID and password.

3.8.3 The IT Customer Service Manager will maintain a list of all approved device accounts and the devices on which they are used.

3.8.4 Physical access to devices that require the use of device accounts in non-public areas (such as workstations used for training) shall be restricted to prevent unauthorized access.

3.8.5 Passwords for device accounts do not expire.

3.9 **Functional Accounts.**

3.9.1 Functional accounts may be requested from the Vice President of ITS to enable ITS staff access when required for system maintenance.

3.9.2 Functional accounts require a unique system ID and password.

3.9.3 Passwords for functional accounts do not expire. However, functional account passwords must be changed annually.

3.9.4 Functional accounts are subject to review and audit.

3.9.5 ITS staff shall log in with their unique individual user ID prior to accessing a system with functional accounts, unless the following conditions exist:

3.9.5.1 A mechanism does not exist for individual authentication.

3.9.5.2 The primary authentication mechanism has failed.

3.10 **Expiring Passwords.**

3.10.1 Each user ID shall have a password associated with it.

3.10.1.1 Each user account must be set up with a “pre-expired” password and the user must be forced to change the password as he/she logs on the first time.

3.10.1.2 Passwords must be changed at least once every 180 days (90 days for system administrator accounts).

3.10.1.3 Passwords cannot be reused for at least 24 cycles.

3.10.2 Passwords shall comply with the following:

3.10.2.1 Passwords must incorporate a combination of upper and lower case letters, and numbers and/or special characters, to ensure an appropriate level of complexity.

3.10.2.2 Passwords must be at least 12 characters (15 characters for system administrator accounts); maximum length is determined by the system restrictions.

3.10.2.3 Passwords cannot be blank.

3.10.2.4 Passwords shall not be obvious or easily guessed (e.g., user ID, user’s name, address, birth date, child’s name, or spouse’s name).

3.10.2.5 Passwords shall not be written down where they may be found.

3.10.2.6 Passwords shall not be shared with other individuals.

3.10.3 Password compliance is subject to review and audit.

3.10.4 Variances to the above will not be granted.

3.11 **Non-Expiring Passwords.** Used for functional or system accounts designated for certain systems or applications to run without the user interaction of having to change passwords.

3.11.1 Non-expiring passwords must adhere to the requirements in Section 3.10 with the following exceptions:

3.11.1.1 Passwords must be reset if there is a threat that the password has been compromised, such as when an administrator leaves the team.

3.11.1.2 Passwords must be at least twelve characters in length.

3.12 **User Sessions.**

3.12.1 All users shall lock the screen when leaving a workstation or laptop unattended.

3.13 **Account Lock Out and Password Reset.**

3.13.1 After five incorrect logon attempts, the user’s account is automatically locked out.

3.13.2 Password resets require authentication of the requesting user. The following authentication/reset methods are permitted:

3.13.2.1 **Telephone.** The reset password may be provided over the telephone once the requestor (Board employee) successfully answers appropriate authentication questions. For a consultant/contractor requesting password reset, the requestor's immediate supervisor must email or call the ITS Solutions Desk stating the employment status of the consultant/contractor. At that point, the ITS Solutions Desk shall assist the consultant/contractor.

3.13.2.2 **In Person.** The reset password may be provided in person once the requestor provides a valid photo ID. This applies to both Board employees and consultants/contractors.

3.13.2.3 **Personal Email.** The reset password may be delivered to an external email address if that email address was initially provided when the account was set up. For a consultant/contractor requesting password reset, the requestor's immediate supervisor must email or call the ITS Solutions Desk stating the employment status of the consultant/contractor. At that point, the ITS Solutions Desk shall assist the consultant/contractor.

3.14 **Account Disabling and Deletion.**

3.14.1 User accounts will be disabled based on any of the following:

3.14.1.1 Authorization from the Vice President of ITS and the Executive Vice President of Administration and Diversity in the event of security concerns.

3.14.1.2 Authorization from the Executive Vice President of Administration and Diversity and the Vice President of HR in the event of potential corrective action, an active investigation, or other HR related issue.

3.14.1.3 Authorization from the employee's supervisor through the online termination process.

3.14.1.4 Authorization from the Technical Manager or Contract Administrator associated with a consultant or contractor.

3.14.1.5 Expiration of the user account.

3.14.1.6 Employee accounts not accessed in 90 days.

3.14.1.7 Non-employee accounts not accessed in 90 days.

3.14.2 Disabled accounts will be retained for six months after which all account contents and history will be deleted. Exceptions are as follows:

3.14.2.1 Extended leave employees (i.e., on military leave, supplemental disability-pay leave, or administrative leave) will only be deleted at the direction of the Executive Vice President of Administration and Diversity or the Vice President of HR.

3.14.2.2 Litigation holds or open records requests involving these accounts.

3.14.2.3 Account Conversion. When a contractor becomes a permanent DFW Board employee, all credentials including network account, active directory account, and associated privileges must be disabled/closed. New credentials with privileges that are in alignment with his/her new job responsibilities must be provided. The same rules apply to a DFW Board

employee becoming a contractor. All credentials, including network account, active directory account, and prior privileges must be disabled/closed. New credentials with privileges that are in alignment with his/her new job responsibilities must be provided.

3.15 **Account Monitoring and Review.**

3.15.1 Technology Security Group must:

3.15.1.1 Review user accounts on a monthly basis.

3.15.1.2 Review user accounts with system administrator access a minimum of one time per month.

3.15.1.3 Review Access to System accounts, Default accounts, Device accounts, and Functional accounts a minimum of one time per year.

3.15.1.4 Conduct periodic searches for unidentified accounts that lack sufficient definition and documentation every six months.

3.15.1.5 Conduct periodic searches for accounts with non-expiring passwords or password expirations above 90 days every six months.

3.15.2 Terminated employee notices will be reviewed and compared to active accounts by the IT Customer Service Manager a minimum of one time per quarter.

3.15.3 ITS Solutions Desk staff must review at a minimum of one time per month:

3.15.3.1 **Disabled Accounts.**

3.15.3.1.1 The terminating manager must notify the ITS Solutions Desk of an employee or consultant/contractor termination. All access to applications for the terminated employee or consultant/contractor must be disabled.

3.15.3.1.2 Ninety days after being disabled, the ITS Solutions Desk shall delete the account and all associated files unless otherwise approved by the Vice President of ITS or designee.

3.15.3.2 Enabled employee and consultant/contractor accounts not accessed in 90 days and shall be disabled.

3.15.4 System logs must be reviewed by the Security Technology Group a minimum of one time per quarter for indications of inappropriate or unusual system activity. Suspicious activity or suspected violations are to be investigated and reported to the Vice President of ITS, the Chief Financial Officer, and the Executive Vice President of Administration and Diversity.

3.15.4.1 System logs must capture sufficient information to identify the event type, date, time, location, source, and origination of an event.

3.15.4.2 System logs must be protected from unauthorized access, modification, deletion, overwrite, or disclosure.

3.15.4.3 Sufficient storage space must be allocated to accommodate storage of system logs to accommodate the scheduled log reviews.

3.15.4.4 System logging and reviewing should be based upon risk and modified as needed.

3.16 **Exceptions.** Exceptions to this policy require the approval of the Vice President of ITS and the Chief Financial Officer with concurrence of the Executive Vice President of Administration and Diversity. Requests for exceptions, along with sufficient justification, must be submitted in writing

by the requesting department head to the Vice President of ITS. Each subsequent request for an exception must stand on its own merit and circumstances without regard to prior exceptions granted**.**

3.17 **Non-Compliance.** Intentional violation of this policy by an authorized user may result in:

3.17.1 Corrective action and/or termination of employment for employees.

3.17.2 Termination of account access for consultants/contractors.

4.0 PROCEDURE

4.1 Not applicable.

5.0 RESPONSIBILITIES

5.1 **Chief Financial Officer and Vice President of ITS**. Authorized to approve exceptions to this policy with concurrence of the Executive Vice President of Administration and Diversity; also responsible for ensuring Board-wide compliance with this policy.

5.2 **Executive Vice President of Administration and Diversity.** Responsible for authorizing requests for user accounts and system administrator accounts to be disabled in the event of security concerns and/or potential corrective action, an active investigation, or other HR related issue.

5.3 **Vice President of HR.** Responsible for authorizing requests for user accounts and system administrator accounts to be disabled in the event of potential corrective action, an active investigation, or other HR related issue; also responsible for ensuring procedures are in place to timely notify the ITS Department of all employee terminations.

5.4 **Department Heads and Supervisors**. Responsible for requesting new access, changes in access, and disabling of access to electronic communication systems for departmental staff and contractors and otherwise complying with PCI related requirements by notifying ITS Department of all employee and consultant/contractor terminations in a timely manner.

5.5 **IT Customer Service Manager.** Responsible for reviewing employee terminations and disabled user accounts for compliance with this policy, responsible for maintaining a list of all approved device accounts and the devices on which they are used, and for reviewing day-to-day processes to ensure compliance.

5.6 **ITS Solutions Desk.** Responsible for processing access requests, authenticating the requestor, and securely providing user ID and password to the requestor.

5.7 **Technology Security Group.** Responsible for monitoring and reviewing accounts, access, rights, privileges, and logs for compliance with this policy and reporting non-compliance to the appropriate management.

5.8 **System Administrators.** Responsible for processing access requests, reviewing access for compliance with this policy, and generating and protecting system logs.

6.0 DEFINITIONS

6.1 **Administrative Authority.** Rights and privileges that allow an individual user to have full access and control of a particular server or system.

6.2 **Authentication.** The process by which a user's identity is verified via a publicly known user ID and a secretly known password.

6.3 **Default Account**. An account that is automatically created through the installation of manufactured software, with a common account name and password used to provide access to administrators and others who must work with the software.

6.4 **Device Account**. An account used to enable access to a device based on demonstrated ongoing need.

6.5 **Electronic Communication Systems.** Includes, but is not limited to:

6.5.1 Computers, computer networks and connections, hardware, software, internal and external storage devices and media, mobile devices (including shared cell phones and Board-issued tablets), two-way radios, two-way text pagers, electronic bulletin boards, fax machines, scanners, cameras (including digital, video, and web), copiers, and modems;

6.5.2 Internet access (including, but not limited to, chat rooms, discussion groups, blogs, and instant messaging); and

6.5.3 Email, voice mail, and all other data information processed and/or produced by such systems regardless of the medium on which the data is stored.

6.6 **Functional Account.** Account used by ITS staff to perform system maintenance. Each account may be utilized by various ITS staff.

6.7 **Least Privilege.** Limiting a user's rights and privileges to the minimum required to effectively fulfill the user's or system administrator's responsibilities.

6.8 **Payment Card Industry Data Security Standard (PCI DSS).** A worldwide information security standard defined by the Payment Card Industry Security Standards Council. Provides an actionable framework for developing a robust payment card data security process – including prevention, detection, and appropriate reaction to security incidents.

6.9 **Root Account**. The "root" account is the most privileged account on a Unix/Linux system. This account gives the ability to carry out all facets of system administration and has no security restrictions imposed upon it.

6.10 **Separation of Duties**. Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.

6.11 **System Accounts.** Accounts used by applications or processes. These accounts are maintained but not used by Application Administrators, Database Administrators, and System Engineers.

6.12 **System Administrator Accounts.** Accounts with elevated privileges to manage specific system information resources. These privileges generally include account provisioning and system configuration and security, and/or access to root accounts.

6.13 **User Account**. Allows a user to authenticate to a system and potentially to receive authorization to access resources provided by or connected to that system.

6.14 **User ID.** Logon ID, user ID, user identification, user account, or any other term used to refer to a user's unique name with assigned resources and privileges. It is utilized to access Board electronic communication systems.

7.0 RESOURCES / FORMS

7.1 **Change Network Access Form.** Online form used to request any modifications to a user's network account, including but not limited to, renewal for expired access, contractor renewal of access request, and permission for access to another drive.

7.2 **Logging and Monitoring Standard.**

7.3 **Related Policies.**

7.3.1 Electronic Communication Systems Usage.

8.0 REVISION HISTORY

8.1 04/01/2005 – IT.003.00 – Original document.

8.2 01/01/2008 – IT.003.01 – Renamed and revised from Network User Administration policy.

8.3 10/01/2011 – IT.003.02 – Added 3.4, 3.5, 3.6, and 3.8; other minor revisions.

8.4 11/01/2014 – IT.003.03 – Added 3.1.3 and 3.1.4; other minor revisions.

8.5 10/01/2015 – IT.003.04 – Revised 3.0; other minor revisions.

8.6 10/01/2018 – IT.003.05 – Renamed from System User and Administrator Access policy; other substantive revisions.