Policy Series 3000
Policy 3005
Procedure 3005.3
Information Technology Services Security Procedure

I. Roles & Responsibilities

1. Protecting customer information is a shared responsibility between NWCCD offices and the Information Technology Services (ITS) staff. Several District offices have procedures and processes in place to manage and reduce risk related to student and employee information.

2. ITS maintains NWCCD procedures and processes that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information. This document is an outline of ITS expectations and practices that protect electronic information.

3. The Colleague Manager's Group members, as outlined in *Procedure 3005.1: Data Security Program*, provides leadership to campus-wide data security efforts and advisory support to ITS staff in these endeavors. This includes the management of the following processes:
   - Maintenance of the *Data Security Training Guide*, which provides a general overview of the District systems, definitions, remote access considerations, and processes for reporting a data breach;
   - Administration of the annual employee training and prevention program;
   - Annual review of the Federal Financial Institutions Examination Council cybersecurity and preparedness assessment; and
   - Development of an annual monitoring report to the NWCCD Board of Trustees that includes preventative activities, risk assessment, data breaches, and future initiatives.

II. ITS Practices/Policies

Access and security to sensitive information comes from a combination of several factors: network security protocols, user credential security permissions, independent system security permissions, and physical restrictions to network infrastructure.

Printed reports containing confidential and sensitive data are secured within offices or behind locked doors. Reports that are no longer needed, containing confidential and/or sensitive data, are shredded or stored securely until they are shredded.

For increased security of information shared electronically, NWCCD has enhanced the email system to identify received emails from external entities. It is also encouraged that the sharing of information be done using OneDrive or the MyNWCCD portal.

In addition to network and physical security, the security access request process is a fundamental layer of protection. This process is key to protecting administrative information and describes the procedures by which system privileges are granted, passwords maintained, security monitored and issues communicated.

System privileges are managed through an ITS process that includes department directors, ITS staff and the Colleague Manager's group members.

Faculty and staff granted access to institutional data may do so only to conduct District business. In this regard, employees must follow *Procedure 3005.1: Data Security Program, Procedure 3005.2: Identify Theft Prevention Program*, the Employee Handbook, and the items contained within this procedure. In summary, employees must:

- Respect the confidentiality and privacy of individuals whose records they access;
- Observe ethical restrictions that apply to the data to which they have access; and
- Abide by applicable laws or policies (e.g., FERPA, HIPAA) with respect to access, use, or disclosure of information.

Furthermore, employees shall not:

- Disclose data to others, except as required by their job responsibilities;
- Use data for their own personal gain, nor for the gain or profit of others; and
- Access data to satisfy their personal curiosity.

Students and employees who violate this procedure are subject to disciplinary procedures managed for students by the Vice President for Student Affairs (*Procedure 5075.2: Student Code of Conduct*) and managed for staff by Human Resources as described in the *Employee Handbook*.

III. Administrative Information

Administrative information is any data related to the business of the District including, but not limited to, financial, personnel, student, alumni, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. Administrative information does not include library holdings or instructional notes unless they contain information that relates to a business function. The District recognizes administrative information as a District resource requiring proper management in order to permit effective planning and decision-making, and to conduct business in a timely and effective manner. Employees are charged with safeguarding the integrity, accuracy, and confidentiality of this information as part of the condition of employment.

Access to administrative systems is granted based on employee need to use specific data, as defined by job duties, and is subject to appropriate approval. As such, this access cannot be

shared, transferred or delegated. Failure to protect these resources may result in disciplinary measures being taken against the employee, up to and including termination of employment.

Requests for release of administrative information are referred to the Public Information Office as outlined in *Policy 3030: Public Records.* The District retains ownership of all administrative information created or modified by its employees as part of their job functions. Administrative information is categorized into three levels:

1. Confidential information requires a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration, or destruction of the data. This includes information whose improper use or disclosure could adversely affect the ability of the District to accomplish its mission.

2. Sensitive information requires some level of protection because its unauthorized disclosure, alteration, or destruction might cause damage to the District. It is assumed that all administrative output from the administrative database is classified as sensitive unless otherwise indicated. Examples include class lists, contract data, and vendor information.

3. Public Information can be made generally available both within and beyond the District. It should be understood that any information that is widely disseminated within the campus community is potentially available to the public at large. Official requests for public records can be made through the NWCCD Public Information Office.

IV. Employee Information

All aspects of personnel records are confidential. Directory information for faculty and staff as published in the NWCCD online Directory is public. Directory information may include some or all of the following: name, department, position title, campus address, campus phone, and email address. All data maintained in the published Directory is also available on-line from off-campus locations. All other employee related data, especially that which is available to users outside Human Resources, such as social security number and birth date, must be vigilantly safeguarded and treated as confidential.

V. Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) of 1974 governs all information about students, current and former, maintained by NWCCD. FERPA generally requires that NWCCD have the student's written permission to release any information from their records except certain types of "directory information."

VI. Student "Directory Information" as defined by FERPA

Certain information, classified as "directory information," is available for public consumption unless the student specifically directs that it be withheld. Current and former students may contact Enrollment Services (or the Records Office) to indicate not to disclose such information. Directory Information as defined by the Act includes: name, address, e-mail, telephone number, campus, program of study, dates of attendance, degrees and awards, date and place of birth, previous school attended, participation in officially recognized sports and activities, and weight and height of athletic team members.

VII. Security process of the central administrative database (i.e., Colleague)

1. Assigning privileges – as noted in Section II, system privileges are managed through an ITS process that includes department directors, ITS staff and the Colleague Manager's group members.

2. Training – members of the Colleague Manager's Group provide leadership to develop required on-boarding materials for all employees who have access to the central administrative database. It is also responsible for on-going training with employees who have access. This includes, but is not limited to, the review of the procedures, updates to security protocols, and standard office procedures as they relate to data security.

3. Modification and Termination
    a. Employees - ITS is notified by Human Resources on employee termination so that the ITS System Administrator can disable all account access.
        i. ITS reviews, monitors, and assesses system logs, including unsuccessful attempts by individuals to access systems which they are not authorized to access. Failed login attempts are logged and alerts are generated to reflect those attempts. ITS will respond immediately to accounts reflecting unauthorized access and will notify department directors of unusual account activity.
        ii. Human Resources immediately notifies ITS of new hires, terminations and changes to employment status (part-time to full-time, etc.).
        iii. Modifications of access are managed by the ITS Process through the Colleague Manager's Group.
    b. Students – ITS is notified by the Registrar on student suspensions and dismissals so that the ITS System Administrator can disable all account access temporarily or permanently depending upon the situation.

4. Passwords and User Login Credentials
    a. Administrative information is protected through the vigilant use of user-defined passwords.
    b. There are minimum password requirements that employees and students must meet. Passwords shall:
        - Be changed by the user every 180 days;
        - Consist of a combination of letters, numbers, and special characters;
        - Be a minimum of 12 characters in length; and
        - Not match previous two passwords or include users' name or username.
    c. Individuals are expected to protect passwords from disclosure including the transmission of passwords through email, instant messaging, etc.
    d. Individuals must have a unique user login.
    e. Sharing of login information with another employee is strictly prohibited.
    f. District login credentials (ie, District email and password) should not be used as a login for any other site or system.