AP 3720-B Local Administrative Permissions to Information Technology Resources

Reference:

17 U.S.C. Section 101 et seq.; Penal Code Section 502, Cal. Const., Art. 1 Section 1; Government Code Section 3543.1(b) ; Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

The District Computer and Network systems are the sole property of the Ventura County Community College District (VCCCD). They may not be used by any person without the proper authorization of the District.

This procedure applies to all District employees and to others granted use of District information resources. This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computers and systems owned, leased, operated, or contracted by the District. This includes desktop computers, laptop computers, and servers, regardless of whether used for administration, research, teaching or other purposes.

Administration of Information Technology: The District has an Information Technology Department (IT) that oversees and is responsible for all district-wide, centralized systems. The colleges each have an IT department that is responsible for local computer resources, including end-user computer systems. The IT groups are responsible for enforcing this procedure.

Computer Permissions Standards: To ensure the highest levels of system integrity and stability, user permissions are structured to grant utilization of installed applications and networked resources. Modification and installation of applications by users is prohibited except under specific conditions. Technical measures to enforce this procedure will include removal of local administrative rights for users.

Conditions for Exception: As a requirement of their staff role or in need to support instructional or research efforts, some users will need to install software in a frequent and recurring fashion to their assigned equipment in order to effectively fulfill their duties. In these situations, the user may request local administrative rights.

If exceptions to the procedure are granted, user's permissions are limited explicitly to the equipment assigned to them. In accepting these privileges the user also accepts an exception to conditions of use, in that correcting problems created by their actions will not be a priority for local support services.

Requests for Exception: Users requesting the implementation of local administrative rights to their computer must complete a request form outlining the justification for this exception, and gain authorization from their Manager and the Information Technology department for their campus.

Implementation: Once exception for local administrative privileges has been granted, a secondary user ID will be generated, and their assigned equipment configured to permit access with this new ID. This ID will take the form of their standard ID with the tag of 'local.' before it; e.g., "local.jdoe." This will be local credentials to their specific equipment. Use of this ID should be explicitly limited to the installation of software, and/or configuration changes necessary, and never used as their day-to-day credentials. Password for this local account must be different from their standard account, and conform to district minimum password standards.

Request for Computer Local Administrative Permissions

Date of Request: _____

Employee Name: _____

Reason(s) for Granting Local Administrative Permissions: _____

By signing this document, the employee acknowledges that they will abide by all terms of this procedure. Failure to do so will result in revocation of local administrative permissions.

Employee Signature: _____

Manager Approval: _____

College Vice President Approval: _____

College Information Technology Approval: _____

District Information Technology Approval: _____