Board Policy No. 440

Information Systems Use Policy

ADOPTED: 1/25/2017	**SUBJECT CATEGORY:** SECTION 400 OPERATIONS
RECENT AMENDMENT: N/A	**SUBSECTION:** INFORMATION SYSTEMS
SEE ALSO: 201, 217, 440A thru 440D	**CONTROL DEPARTMENT:** INFORMATION SERVICES

I. PURPOSE

The purpose of this policy is to outline the acceptable use of information systems and resources at AC Transit. Inappropriate use exposes AC Transit to risks including malware, compromise of network systems and services, and legal issues. Therefore, this policy has been put into place to protect users and the District.

II. PERSONS AFFECTED

All users of the District's computers or network infrastructure.

III. DEFINITIONS

"Data" is any and all information stored or transmitted over AC Transit resources.

"Information System" refers to all resources that store, transmit or present information related to AC Transit business.

"Resources" refers to all District-owned hardware and software including, but not limited to:

- Computers, laptops, mobile devices, tablets, desk phones
- Network storage, network infrastructure, servers
- All software applications licensed by the District
- Accounts such as email accounts or other accounts used to access District applications
- Data plans, subscription services

"Sensitive information" includes all data, in its original and duplicate form, which contains personal information, protected health information, customer record information, card holder data, confidential personal data, or information that is deemed to be confidential or is otherwise exempt from disclosure under state law.

"User" is anyone using District computing resources including, but not limited to, employees; contractors; consultants; limited-term employees; interns; Board Officers and Board Members.

IV. POLICY

A. Acceptable use

Use of AC Transit's information systems is limited to District business consistent with Board Policy 217, Use of District Resources.

B. Strictly Prohibited Use

1. Use of AC Transit's information system to send messages of a threatening, harassing, or obscene nature, or any behavior found to be inconsistent with Board Policy, is prohibited. (See also Board Policy 201, Anti-Bullying and Prevention of Abusive Conduct.) Inappropriate use may include, but is not limited to, the display or transmission of sexually explicit images, messages or cartoons; or any transmission that contains ethnic slurs, racial epithets or anything that constitutes harassment or disparagement of others based on their race, national origin, color, sex, sexual orientation, age, disability, religious or political beliefs.
2. With the exception of Information Services (I.S.) staff, users are prohibited from connecting any computer or network device to the local area network (LAN). This includes network interface cards, access points, routers, and switches.

C. Security and Personal Information

1. All software applications and subscription services are to be secured with a password sufficient to protect District information. Users who are granted access to any part of the information system are provisioned with an account.
2. Users are to use their assigned account(s) and no other.
3. Users are prohibited from using another user's account to access any part of an information system.
4. Users are prohibited from sharing their passwords or passphrases.
5. Authorized District staff may reset passwords as required for business purposes.
6. Users who are provisioned with District resources are not allowed to modify them. Unless directed to do so by authorized Information Services personnel, they may not change permissions, modify hardware, or modify code and configuration on any District resource.
7. All users are responsible for safeguarding sensitive information. Users may access, use or share sensitive information held by the District only to the extent it is authorized and necessary to fulfill their assigned job duties.
8. Users must immediately notify I.S. staff if sensitive information is inappropriately shared or exposed.
9. Users must immediately report to I.S. staff any suspicious e-mail or other computer activity.

D. No Expectation of Privacy

1. AC Transit owns all data stored on District resources and reserves the right to access anything the user has viewed or created using those resources.
2. Users shall have no expectation of privacy. Authorized District staff may view any and all activities and any data created, stored or transmitted using District resources. They may access any electronic data or files at any time without consent from or notification of the user.

3. The District may monitor, record and review any data or websites a user may have accessed through a District Internet connection.
4. The District strongly discourages the storage of personal files and messages (pictures, personal email, texts, instant messages, music, spreadsheets, etc.) on District-provided computers. All such data may be accessed and reviewed at the District's discretion and may be deleted without notice.

V. AUTHORITY

A. General Manager's Authority

The General Manager is directed to implement the necessary Administrative Regulations and controls regarding computer hardware and software, information security, e-mail use, and mobile devices to implement this policy.