Board Policy No. 440

Information Systems Use Policy

ADOPTED: 1/25/2017 **RECENT AMENDMENT:** 5/11/22 **SEE ALSO:** 201, 217, 440A, 440B, 440C, 440D	**SUBJECT CATEGORY:** SECTION 400 OPERATIONS **SUBSECTION:** INFORMATION SYSTEMS **CONTROL DEPARTMENT:** INNOVATION AND TECHNOLOGY

I. PURPOSE

Inappropriate use of the District's technology resources exposes the entirety of our transit district's infrastructure to malware, ransomware, data loss, compromise of network systems and services, business disruptions and legal liability. This policy outlines the District's expectations of authorized users regarding the acceptable use of IT information systems and resources. This policy equally establishes parameters for the individual use of all IT systems and resources under the control of the District.

II. PERSONS AFFECTED

This policy applies to all District Board Members, Board Officers, employees, contractors, consultants, temporary employees, and interns.

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 District information.

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

- Computers, laptops, mobile devices, tablets, smart phones, desk phones, badges
- Cameras, Fare equipment, network sensors
- Network storage, network devices, network infrastructure, servers
- All networks of landline, wireless, cellular, radio, and satellite
- All software applications licensed and subscribed by the District
- Accounts such as email accounts or other accounts used to access District applications
- Data plans, subscription services, online services, cloud subscriptions

"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 Information Systems and 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. It is the responsibility of each Board member, Board Officer, District employee, contractor/vendor representative, and any other person or entity operating under the direction of the District to ensure that his or her work behavior and performance comply with this policy and all other District policies, including Board Policy 201, Anti-Bullying and Prevention of Abusive Conduct and Board Policy 213, Prohibiting All Forms of Unlawful Employment Discrimination, Including Sexual or Other Forms of Harassment when using District Resources.
2. Users are prohibited from connecting a non-District owned computer or network device to the District networks. This includes but is not limited to cameras, access controllers, network sensors, network interface cards, access points, routers, and switches. Any exception to this policy requires a written request and approval by the Chief Information Officer.

C. Security and Personal Information

1. All software applications and subscription services are to be secured with a strong password sufficient to protect District information. Users who are granted access to any part of the information system are provided an account.
2. Users must use their assigned account(s) without exception.
3. Users are expressly prohibited from using another User's account to access any information system.
4. Users are prohibited from sharing their passwords or passphrases.
5. Users must use Multifactor Authentication (MFA) access technology where required.
6. Authorized District staff may reset User passwords for required business purposes.
7. Users who are provided District resources are not permitted to make any modifications, unless directed to do so by authorized IT personnel.
8. Users may neither change permissions, modify hardware, nor code or configurations of any District resource.
9. 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.
10. Users must immediately notify the IT Help Desk when sensitive information is inadvertently shared or exposed.
11. Users must immediately report any suspicious e-mail or other computer activity to IT Help Desk.

D. No Expectation of Privacy

1. AC Transit owns all data stored on District Resources and reserves the right to access any content viewed or created using District 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. Authorized staff members may also access any electronic data or files at any time without consent or prior 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 expressly discourages the storage of personal files and messages (pictures, personal email, texts, instant messages, music, spreadsheets, etc.) on District-provided resources. Personal data may be accessed and reviewed at the District's discretion and may be deleted without notice.
5. All activity related to AC Transit business may be subject to California Public Records Act requirements, regardless of whether conducted on District Resources or a personal device.

E. Remote Access

a. Users shall contact the IT Help Desk for approved methods and software to remotely connect to District Information Systems and Resources.
b. Remote access Users are responsible for ensuring their mobile device is compliant with this Policy and Administrative Regulation 440B.
c. All devices may be assessed by the District IT Department prior to use to ensure the device has updated and applicable security patches and virus/malware protection software.
d. Users with remote access privileges shall ensure that their remote access connection is used explicitly for work business and used in a manner consistent with their onsite connection to the District network.
e. Remote access connection shall not be used on a personal device, unless a written request is reviewed and approved by the Chief Information Officer.

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.