

RESOLUTION NO. 2019-04

**A RESOLUTION OF THE MASON TRANSIT AUTHORITY BOARD
ADOPTING A REVISED INFORMATION TECHNOLOGY ACCEPTABLE USE
POLICY (POL-702).**

WHEREAS, pursuant to Resolution No. 2014-37, Mason Transit Authority adopted an Informational Technology Acceptable Use Policy establishing and defining the terms, conditions and rules regarding use of MTA's information technology resources by employees; and

WHEREAS, since the adoption of that resolution, additional provisions to protect the integrity of the information technology resources, as well as minor edits and clarifications in the policy will bring the policy current;

NOW THEREFORE, BE IT RESOLVED BY THE MASON TRANSIT PUBLIC TRANSPORTATION AREA AUTHORITY BOARD that the revised Information Technology Acceptable Use Policy (POL-702), which is attached hereto and incorporated herein, be established and adopted.

Adopted this 19th day of March, 2019.



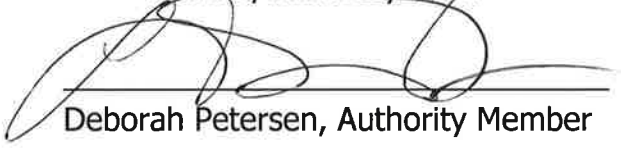
Randy Neatherlin, Chair



John Campbell, Authority Member



Sharon Trask, Authority Member



Deborah Petersen, Authority Member



Sandy Tarzwell, Authority Member


Wes Martin, Vice-Chair



Kevin Dorcy, Authority Member




Kevin Shutty, Authority Member



Don Pogreba, Authority Member

APPROVED AS TO CONTENT: 
Danette Brannin, General Manager

APPROVED AS TO FORM: 
Robert W. Johnson, Legal Counsel

ATTEST:  DATE: 3/19/19
Tracy Becht, Clerk of the Board



Title:	Information Technology Acceptable Use
Number:	702
Effective:	January 1, 2015, REVISED March 19, 2019
Cancels:	N/A
Prepared by:	Josh Jacobs, Systems Administrator
Approved by:	Authority Board Resolution No. 2014-37; Resolution No. 2019-04

POL-702 INFORMATION TECHNOLOGY ACCEPTABLE USE

This policy defines the acceptable use of Mason Transit Authority's (MTA) information technology (IT) resources.

1. Authorized Users

All MTA employees who are assigned a domain login are authorized to use MTA IT equipment. MTA employees are expected to keep their login credentials secure and to use their own login. Using another employee's login is not permitted at any time for any reason. Sharing your password with anyone, including IT staff, is not permitted. Users will lock or log out of their computer any time they are away from their desk. Users are responsible for all actions done with their account. All activity done on the network is monitored and recorded for security auditing purposes. Failure to maintain accountability of your domain login may result in disciplinary action, including but not limited to reimbursement to MTA for damages/loss of equipment and/or termination.

2. Data

All data and files originating by users of MTA's IT equipment are considered property of MTA. Data originating from or received by users of MTA's network is not considered private. MTA reserves the right to access, monitor, examine, copy, modify, delete, or share all data on IT resources without notice.

3. Public Records

All activities done on or data created with MTA equipment and resources, or while conducting MTA business, are subject to the Public Records Act (RCW 42.56). It is the responsibility of the creating user or team of the data to keep and maintain their data in accordance with RCW 40.14, Preservation and Destruction of Public Records.



Title:	Information Technology Acceptable Use
Number:	702
Effective:	January 1, 2015, REVISED March 19, 2019
Cancel:	N/A
Prepared by:	Josh Jacobs, Systems Administrator
Approved by:	Authority Board Resolution No. 2014-37; Resolution No. 2019-04

4. Authorized Devices

Only computers and devices approved by the Systems Administrator are authorized to be placed on the network. MTA staff is not permitted to move MTA computers or devices without the Systems Administrator's approval.

5. Authorized Software

Employees may not install software on MTA computers operated within the MTA network. A software request must first be approved by the requester's manager, then it is sent to the Systems Administrator through the ticket system. Software must be approved by the System Administrator. The Systems Administrator will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation. Installing unauthorized software may result in disciplinary action, including but not limited to reimbursement to MTA for damages/loss of equipment and/or termination.

6. Password Security

All domain user accounts will be subject to password security policies.

- Passwords will expire 90 days after being created.
- New passwords cannot contain a user's name.
- New passwords cannot be the same as the last 10 passwords.
- Passwords must meet the following complexity requirements.
 - Must be at least 10 characters long.
 - Must meet 3 of the 4 conditions:
 - 1 lowercase letters.
 - 1 uppercase letters.
 - 1 numbers.
 - 1 symbols.
- Domain accounts will be locked after 3 failed password entries within 5 minutes.
- Locked out accounts will be locked for 5 minutes.



Title:	Information Technology Acceptable Use
Number:	702
Effective:	January 1, 2015, REVISED March 19, 2019
Cancels:	N/A
Prepared by:	Josh Jacobs, Systems Administrator
Approved by:	Authority Board Resolution No. 2014-37; Resolution No. 2019-04

Service accounts will be exempt from this password security policy. Administrator account passwords will expire every 30 days.

7. Provision of IT Equipment

MTA, at its discretion, may provide IT resources in the form of equipment to employees for their use in fulfillment of their job responsibilities. In receiving the equipment, the employee acknowledges and accepts responsibility for the proper care and secure storage of the assigned equipment while it is in their possession. Failure to uphold these responsibilities may result in disciplinary action, including but not limited to reimbursement to MTA for damages/loss of equipment and/or termination.

8. Common Area Computers

Common area computers are designated for personal use while on breaks. Employees may check personal e-mail or browse personal websites. Except as explicitly provided herein, employee's use of common area computers is subject to all MTA rules and policies including section 10. These computers are a privilege that MTA can revoke at any time for any reason.

9. De minimis Use for IT Equipment

De minimis, or infrequent or occasional use that results in no actual cost to the agency, is permitted on MTAIT equipment. De minimis use will be regulated by the employee's immediate supervisor. At the supervisor's discretion, de minimis computer use can be prohibited. Such prohibitions must be made in memorandum format and kept on record until changed or revoked. De minimis use must comply with all other sections of this policy and other applicable policies.

10. Acceptable Uses for IT equipment

MTA's IT equipment is to be used in the context of a professional business environment. MTA expects users to be respectful, lawful, and ethical in their use of IT equipment and resources. Any use of IT equipment or resources that violates



Title:	Information Technology Acceptable Use
Number:	702
Effective:	January 1, 2015, REVISED March 19, 2019
Cancels:	N/A
Prepared by:	Josh Jacobs, Systems Administrator
Approved by:	Authority Board Resolution No. 2014-37; Resolution No. 2019-04

MTA's policies is strictly prohibited and may incur disciplinary action relative to the infraction including termination.

The following are examples of prohibited conduct; this list is not all inclusive:

- Transmitting, viewing, downloading, posting or exchanging defamatory, obscene, offensive, pornography, discriminatory, harassing, or threatening content in documents or images.
- Using MTA's time and resources for personal financial gain.
- Acquiring, using, or disclosing someone else's login credentials.
- Violation of Copyright and/or Intellectual Property Rights laws.
- Violation of State and Federal Privacy Laws such as the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA) pertaining to unauthorized use or release of Personally Identifiable Information (PII).
- Failing to observe licensing agreements.
- Installation of any software without the explicit authorization of MTA's System Administrator.
- Engaging in unauthorized transactions that may incur a cost to MTA or initiating unwanted Internet services and transmissions.
- Participating or attempting to participate in the transmission, viewing downloading, posting or exchange of pornography or obscene materials.
- Attempting to gain unauthorized access to the network or computer system of another organization or individual.
- Transmitting or posting chain letters or solicitations. (Except on common area computers)
- Using the Internet for political or religious causes or activities, or any sort of gambling.
- Representing personal views as those of MTA.
- Sending anonymous e-mail messages.
- Engaging in any other illegal, fraudulent, or malicious activities.