AECOM Global

End User Acceptable Use Policy

T1-002-PL1

1. Purpose and Scope

AECOM and its subsidiaries and affiliates (collectively AECOM or the Company) rely on employees to perform normal business operations and provide services to clients. This policy is intended to define the acceptable and prohibited use of the AECOM technology resources along with the end-user responsibilities for protection of these assets. This policy is intended to promote responsible use of AECOM resources and protect the Company and its employees, clients, and other parties, from inappropriate disclosure of confidential information, Restricted and Highly Restricted Information, loss of competitive advantage, loss of productivity, damage to reputation, exposure to civil and criminal liability, and inability to meet client and contractual obligations.

This policy sets forth the requirements for responsible and secure use of, and ownership and access to, AECOM technology resources and applies to all end-users. All AECOM end-users shall adhere to requirements defined in this policy.

Any use, possession of, or access to AECOM Technology Resources constitutes acceptance of and consent to the terms of this End User Acceptable Use Policy – AECOM Global.

2. Policy

2.1 Ownership

The Company retains ownership of AECOM Technology Resources. Users' access to and use of AECOM Technology Resources is at the will and discretion of the Company, and the Company reserves the right to prohibit or limit users from accessing or using AECOM Technology Resources at any time for any reason.

Without limitation to the foregoing, the Company is and remains the owner or custodian of all information created by the Company's employees and other users during their relationship with the Company relating to the business and services of the Company, no matter where such information is created, stored or maintained.

While the Company reserves the right to and intends to retain communications and other records in accordance with Company record retention policies and procedures and its legal obligations, users acknowledge communications and information stored in the AECOM Technology Resources may be deleted or destroyed at any time, including as an exercise of Company discretion or as result of system or other failure.

Under no circumstances is an employee of AECOM authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing AECOM Technology Resources.

2.2 Personal Privacy and Right to Monitor

No Expectation of Privacy. To the fullest extent allowable by applicable law, users do not have any expectation or right to privacy in their use of AECOM Technology Resources or any communications or other information stored on, transmitted by, or received through AECOM Technology Resources.

AECOM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. For security and network maintenance purposes, authorized individuals within AECOM may monitor equipment, systems and network to track compliance.

2.3 Access Management

a. Access credentials including passwords, PINs, and AECOM issued badges shall be protected.

b. Passwords shall not be written down or stored in clear text and shall meet user account password requirements. See the Password Standard for requirements.

c. User accounts and passwords shall not be revealed or shared with others, including technical support personnel, co-workers, family members or other household members when working from home.

d. Users shall not ask others for their credentials.

e. Computer screens shall be locked when left unattended.

2.4 Asset Management

a. Equipment shall only be procured or requested through AECOM from official corporate sources supported by your regional IT office. Mobile devices owned by users (i.e., BYOD) are allowed.

b. Equipment shall be returned to AECOM on the users last working day in the office or within 30 days from date of termination/separation for remote users.

c. Laptops and any other mobile and storage devices shall not be stored in unsecured areas.

d. Workstations shall be connected to the corporate network at least monthly to receive updates, and if prompted, have a system reboot performed as necessary. VPN connection is acceptable for connection to the corporate network.

e. Users are prohibited from using the AECOM Technology Resources in connection with any illegal activity or to transmit, display, store, publish or receive any illegal, pornographic, obscene, sexually explicit or otherwise inappropriate material.

f. Users are prohibited from using the AECOM Technology Resources in connection with any activity that infringes on third-party intellectual property rights. This includes without limitation prohibitions on using any software that is not licensed for the conditions under which it is being used and on using unauthorized software or reproducing software in violation of applicable license agreements. Users shall use all software in accordance with the terms of the applicable license agreements. Company software is intended to be used only on Company-supported computers.

g. Users shall not attempt to bypass firewalls, circumvent monitoring, disguise identity or bypass security controls through the use of anonymous proxies, or any unauthorized network or Internet connection, or any other means or engage in any other activity that may cause harm or damage to any Electronic Communications System or Company Information.

h. Use of unauthorized hardware or connecting unauthorized hardware or devices to the network is prohibited. Without limitation to the foregoing, users are prohibited from connecting remotely to the network except in compliance with the Remote Access and VPN Standard – AECOM Global.

i. Users are prohibited from deliberately performing acts which waste computer resources. This includes personal use of the Internet to play games, participate in virtual worlds, to download large files that are not business related, or listen to streaming audio or watch streaming video that is not business related.

j. Users shall not disable or reconfigure security controls such as antivirus, personal firewalls, or encryption if installed on a Company computer.

2.5 Mobile Devices

This section pertains AECOM issued / owned mobile devices.

a. Mobile devices shall be kept up-to-date with manufacturer patches.

b. Users shall not load pirated software or illegal content onto AECOM issued mobile devices.

c. Mobile devices shall be configured with a secure password.

d. Mobile devices shall not be "jailbroken" or have any software installed which is designed to gain access to functionality not intended to be exposed to the user.

e. Mobile devices shall not be connected to a PC/Laptop which does not have up-to-date anti-malware protection.

2.6 Internet and Communication Applications

2.6.1 Internet

a. Users shall not violate any laws or regulations through use of AECOM Internet resources.

b. Users shall be accountable for all Internet activity associated with their accounts and therefore, users shall not allow others to access the Internet by using their accounts.

c. Users shall not save user-ids and passwords using cookies or other means for non-AECOM applications and sites.

2.6.2 Email Usage

a. AECOM email accounts shall be used for business related purposes only and usage shall comply with the Email Standard – AECOM Global.

b. User shall report any suspicious emails to abuse@aecom.com.

c. AECOM email shall not be forwarded automatically to a third-party email system and storage servers such as Google, Yahoo, and MSN Hotmail etc.

2.7 Software Usage

a. Users shall not download, install or run any unauthorized, malicious or potentially malicious programs (e.g., viruses, worms, trojan horses etc.) on any AECOM Technology Resources.

b. Users shall not install software obtained from non-AECOM sources on AECOM Technology Resources unless approved by Information Security.

2.8 Network Usage

a. Users shall not extend, re-transmit or alter network components in any way to access AECOM information with willful or malicious intent.

b. Users shall not download, install or run security programs or utilities (e.g., NMAP, Wireshark etc.) without prior approval of IT Management and Information Security.

2.9 Information Protection

a. Individual users are responsible for understanding and adhering to information classification standards and procedures to protect information based on its classification.

b. Each user may only handle information that is relevant to performing their assigned job function(s).

c. Users shall not store Restricted or Highly Restricted information on non-AECOM owned devices or systems such as personal USB drives, laptops or cloud storage solutions (e.g. Dropbox, Google Drive etc.).

d. Users shall not transmit (e.g., email, upload etc.) or store Restricted or Highly Restricted information for non-AECOM business related purposes.

e. Users shall apply appropriate means of disposal for information based on classification, such as using a paper shredder to dispose of documents containing Highly-Restricted information.

f. Unauthorized acts of destruction or disclosure of AECOM data by any means is prohibited.

3. Compliance with Regulations

a. Individual users are responsible for understanding their role in adherence to their applicable state, government and international laws and regulations.

b. Users shall not violate applicable software licensing and copyright laws and are responsible to be informed of updates to remain compliant accordingly.

4. Incident and Misuse Reporting

a. Actual or suspected security incidents (e.g., phishing attack) or misuse of AECOM Technology Resources shall be reported promptly by users to the IT help desk or abuse@aecom.com.

5. Policy Compliance

5.1 Effective Date

This End User Acceptable Use policy is effective as of 24 May, 2019. As of such date, it supersedes any prior policies and procedures or parts thereof that address the subject matter herein.

5.2 Compliance Measurement

The Information Security team will verify compliance with this policy through various methods, including but not limited to, security tool reports and internal / external audits. Feedback from reports and audits will be provided to the policy owner.

5.3 Exceptions

Any exception to this policy shall be approved by the Information Security team.

5.4 Enforcement

Users who violate the terms of this policy may be subject to discipline, up to and including termination of employment, and any applicable criminal and/or civil penalties. The Company may also terminate access to the AECOM Technology Resources for users who violate this policy.

5.5 Minimum Requirements

This firm-wide policy specifies minimum requirements. All AECOM entities are required to meet or exceed the requirements of this firm-wide policy and may, with appropriate approval, add local IT policies to meet unique business, environmental or legal requirements, provided their local IT policies do not conflict with, and are not less stringent than this policy.

6. Acknowledgement

a. Users expressly waive any right of privacy in anything they create, store, send or receive on AECOM Technology Resources.

7. Terms and Definitions

a.	**AECOM Technology Resources**	All computer hardware and software, network elements, systems, cloud applications and infrastructure, communication devices, and other devices, equipment, or software and supporting utilities and services owned by AECOM or otherwise used for AECOM business. This includes without limitation email systems, voice mail, and other electronic messaging systems; mobile and wireline telephones, telephone systems, and long-distance services; electronic devices and storage systems, such as modems, computers, tablets, handheld devices, hard disk drives, removable drives, tapes, and data and storage systems; software, networks, intranets, websites, and AECOM owned, leased or rented Internet based sites/applications/services; and facsimile machines.
b.	**Users / End-Users**	Users are named resources with whom AECOM shares its information which includes, but not limited to: Employees, contractors, joint venture partners, interns.
c.	**Public Information**	This data has been specifically approved for public release by Public Relations department or Marketing Department Managers. Unauthorized disclosure of this information will not cause problems for AECOM, its customers, or its business partners.
d.	**Internal Information**	This data is related to the day-to-day operations of AECOM. Unauthorized disclosure of this information would have minimal to no impact on the confidentiality, integrity or availability of resources for AECOM, its customer or its business partners.
e.	**Restricted Information**	This data is sensitive and intended for use within AECOM, and in some cases within affiliated organizations, such as AECOM partners and customers. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may negatively impact AECOM, its customers, or its business partners.
f.	**Highly Restricted Information**	This data is protected by law, regulation and includes customer data. If this information is lost, disclosed, or inappropriately modified, this could cause significant adverse impact to the confidentiality, integrity, availability of resources for AECOM its customers or its business partners.

8. References

a. Information Classification Policy- AECOM Global T1-401-PL1

b. Password Standard – AECOM Global T1-101-PR1

c. Email Standard – AECOM Global T1-300-PR1

d. Remote Access and VPN Standard – AECOM Global T1-104-PR1

e. Media and Data Standard – AECOM Global T1-103-PR1

f. Records Management Retention Procedure – AECOM Global Q1-004-PR1

9. Records

a. Security tool reports and internal / external audits.

10. Change Log

Rev #	Change Date	Description of Change	Location of Change
0	13-Jul-2016	Initially released as Electronic Communications Policy – AECOM Global T1-400-PL1	
1	24-Mayr-2019	2019 Review; re-released as End User Acceptable Use Policy – AECOM Global T1-002-PL1	All