TRANSPORTATION TECHNOLOGY ACCEPTABLE USE AGREEMENT (AUA)

Acceptable Use Agreement (AUA) – Consultant/Outside Agency

1. Background, Purpose, and Scope:

Information assets owned by the Florida Department of Transportation ("FDOT" or the "Department"), including but not limited to FDOT data and information, computing devices, cell phones, and removable storage devices, are strategic assets intended for official business use only and are entrusted to staff for the performance of their job-related duties. The scope of this policy extends to all Information Technology Resources owned or operated for FDOT-related business and to all employees, consultants/contractors or other personnel (referred to as staff) authorized to use these Information Technology Resources ("Authorized Users"). All Authorized Users must use and protect FDOT information assets and resources in accordance with this policy and applicable information security and privacy policies.

Authorized Users are responsible for systems security to the degree that his or her job requires the use of information and associated systems. All Authorized Users are responsible for using information resources only for the purposes for which they are intended, to comply with all controls established by information resource owners and custodians, and for protecting sensitive information against unauthorized disclosure.

2. General Use:

a. Use of Computing Devices: Computing devices that connect to the FDOT network must be properly protected with the most current software and updates available to ensure that data exchanged is not compromised and does not contain viruses or malware.

Non-FDOT computing devices used for FDOT business purposes, such as but not limited to e-mail, must be made available for audit and inspection and is subject to Public Records Requests.

All FDOT-related information must be removed from non-FDOT computing devices when employment or a contract is terminated with FDOT.

b. Passwords and Personal Information: Information, methodologies or devices used for authentication and authorization purposes (passwords, Personal Identification Numbers [PIN], security questions/answers, security tokens [e.g., smartcard, key fob]) must remain confidential.

c. Badges: Authorized Users are responsible for safeguarding their ID Access Badge. Lost or stolen ID Access Badges must be reported immediately to the FDOT Service Desk at FDOT.ServiceDesk@dot.state.fl.us. Guests or staff without a badge must go to the lobby to obtain a guest or temporary badge. Badges must always be worn and kept visible at all FDOT locations. Badges must be safeguarded and stored in a private location after hours.

3. What Constitutes Acceptable Use:

a. Authorized Users accessing Department Information Technology resources are expected to act in good faith and take reasonable steps to avoid abuse and inappropriate use of resources.

b. Any personal use of the internet and/or email must be brief, infrequent, and in compliance with the Department's policies.

c. Public Wi-Fi is provided for use during lunch and scheduled breaks in breakrooms located at the district headquarters main building in all districts.

d. Bring Your Own Device (BYOD): FDOT provides a guest Wi-Fi network for consultants, contractors, outside agencies and vendors when performing duties on behalf of the Department.

The owner of the equipment is entirely responsible for their own hands-on support and hardware and assumes all risks and liabilities. The Service Desk may provide limited hands-off support.

When connected to the FDOT guest Wi-Fi network, the device owner may connect to the production network using Hayes VPN.

Lost or stolen BYOD devices, which are used to perform Departmental business, must be reported to the FDOT Service Desk immediately.

4. What Constitutes Unacceptable Use:

a. Passwords and Confidential Information: An Authorized Users's password must not be displayed, printed, emailed, recorded in an unsecured manner, stored in a web browser, or shared with anyone else.

The password for password-protected external drives must not be shared with unauthorized individuals.

FDOT confidential or exempt information must not be stored on any non-FDOT device without explicit permission or authorization.

Personal or confidential information must not be sent using text messages.

b. Internet and Social Media: Authorized Users may not discuss or disclose Department business on social media. Although Authorized Users are permitted to share content originating from official FDOT social media accounts, Authorized Users must not post any other content related to Department business on their personal or non-FDOT social media. When reposting official Department content, Authorized Users may not alter the contents of the original post.

Inappropriate use of the internet for sites related to pornography, gambling, or for a personal business may result in disciplinary actions up to and including dismissal, termination of contracts, or other legal action.

c. FDOT Business-Related Email: Authorized Users must not use personal email accounts to conduct FDOT business or enable rules to auto-forward e-mails and calendar appointments from their FDOT e-mail address to non-FDOT e-mail addresses.

d. Badges: Tailgating, or the use of another staff member's ID Access Badge (authorized or unauthorized), is not permitted and badges must not be left unattended or in plain view when not in use.

e. Hardware and Software: Unauthorized or prohibited hardware and software are not permitted to be installed on FDOT resources.

Software used to intercept or monitor network traffic is strictly prohibited unless authorized by the Information Security Management Office.

Authorized Users must not attempt to circumvent security controls that have been implemented, including but not limited to the firewall, VPN, end point protection, and computer device management software. Doing so may result in revocation of access or other disciplinary actions up to, and including, dismissal, termination of contracts, or other legal action.

FDOT owned or managed computer technology may not be taken out of the United States without approval from the Information Security Manager (ISM).

FDOT data and systems that must be accessed with a userid and password may not be accessed from outside of the United States without approval from the ISM.

f. It is not permissible for Department staff to connect personal devices to the FDOT guest Wi-Fi network.

5. Reporting Security Incidents or Breaches of Security:

Security incidents and breaches of information, whether confirmed or potential, and lost or stolen computing devices must be reported immediately to the FDOT Service Desk at FDOT.ServiceDesk@dot.state.fl.us. Any suspected or actual activities and/or events indicating misuse or violation of this Acceptable Use Policy must be reported immediately to the Information Security Management Office at ISM@dot.state.fl.us.

6. Enforcement:

Misuse or abuse of any Information Technology Resource, including e-mail, Internet access, and social media sites by any member of the Department's workforce may result in the revocation of access and other disciplinary actions up to and including dismissal, termination of contracts, or other legal action. By executing this Agreement, all Authorized Users acknowledge that state and/or federal law may impose criminal penalties for certain computer related acts that may also constitute violations of this policy.

There is no expectation of privacy in the use of Information Technology Resources provided by the Department such as internet, e-mail, mobile and computing devices, etc. Random reviews of e-mail and internet usage are conducted to detect abuse or misuse of FDOT resources. Data generated by staff is subject to Public Records Requests. This includes things such as documents, emails, text messages and instant messages.

7. Waiver and Exceptions:

Exceptions to standards and written policies must be requested in writing through the Information Resource Request (IRR) application except where alternate processes are defined.

8. Definitions and Terms:

Enterprise Business Glossary

9. Certification:

I will comply with Department policies stated herein and all applicable state and federal regulations related to Information Technology Security. I will not use my access in any improper or unauthorized manner. I understand that failure to comply with this Acceptable Use Agreement may lead to disciplinary action up to and including termination of employment, termination of contracts, or other legal action. I certify that I have read and completed the following:

- Policies and Procedures Regarding Information Technologies
- Computer Security Awareness CBT (attach copy of certificate)

SIGNED:

Consultant/Outside Agency User **Date** | **Printed Name**

Consultant Company or Agency Name | **FEIN/Tax ID #**

Email Address | **Phone**

Have you ever previously worked with or for FDOT? Yes ☐ No ☐

TRANSPORTATION TECHNOLOGY ACCEPTABLE USE AGREEMENT (AUA)

To be completed by the user's **company manager** or **outside agency** contact.

Company Manager or Outside Agency Contact Signature

Date

Company Manager or Outside Agency User Name

Phone

Company Manager or Outside Agency Contact Title

Company Manager or Outside Agency Contact Email Address