GATEWAY PROGRAM DEVELOPMENT CORPORATION
COMPUTER USE AND SECURITY POLICY

I. Introduction

This document sets forth the official policy of Gateway Program Development Corporation (GDC) relating to the acceptable use of GDC's information technology resources, including but not limited to equipment, software, networks, data and stationary and mobile communications devices whether owned, leased or otherwise provided or authorized for use by GDC.

II. Policy

This policy describes the terms, conditions and requirements that govern (1) the use of GDC's computing and communications hardware and software (components of which, including GDC's network, are referred to individually and collectively herein as "GDC's System"); and (2) use of computing devices to enable authorized creation, access, retrieval, transmission or storage of information to, from or on GDC's System for purpose of conducting GDC-related business; and (3) management of GDC electronically stored information.

Improper or unauthorized use of the GDC's System, or the information it contains, could subject GDC to legal liability, financial loss and reputational harm. This policy has been established in order to: (1) protect the confidentiality, integrity, and availability of GDC information; (2) protect GDC's management, staff, and Project Partners (NJ Transit, Amtrak and Port Authority of New York and New Jersey) from the risks associated with the improper use of GDC's System and; (3) help insure that GDC's System operates in a reliable, responsive, and efficient manner.

III. Scope

This policy applies to all GDC Trustees, management, staff, employees, contractors, consultants, or other third parties working for or on behalf of GDC ("User" or "Users"). GDC's System is comprised of, and this policy covers, all computing and communications hardware and software owned or leased by GDC.

In addition, this policy applies to all computing devices, such as smartphones, tablets, laptops, or desktops, used to access, directly or remotely, any information on GDC's System or software or other elements of GDC's System, and to any GDC information stored outside of GDC's System.

IV. Compliance

By, in any manner, directly using GDC's System, or by using a personally owned or GDC-owned or leased device to access remotely information on, or software or other elements of, GDC's System, the User acknowledges that he or she understands, accepts and will comply with all of the terms, conditions and requirements of this policy. Failure to comply with this policy may result in the temporary or permanent restriction or denial of a User's access to GDC's System, and the remote deletion of GDC information from User-owned, or GDC-owned or leased remote access computing devices. In addition, GDC, in its sole discretion, may undertake disciplinary action, including possible termination and pursuit of civil or criminal legal action.

This policy sets forth the minimum standards for Users regarding security of GDC's System. Applicable law or GDC's Project Partners may require GDC and Users to apply different or additional standards or impose different or additional requirements regarding certain information and data, and in such cases, Users shall comply with those standards and requirements that exceed the minimum standards set forth herein.

V. Use of GDC's System

A. User Responsibilities and Expectations.

1. Personal Use. GDC's System is provided to assist Users in the performance of GDC business. Users should exercise good judgment regarding any limited use of GDC's System for personal non-business related purposes. Occasional, limited, personal use of GDC's System is permitted if such use does not (a) interfere with the User's or any other person's job performance; (b) have an adverse effect on the performance of GDC's System; or (c) violate any guidelines, standards or policies of GDC. Personal use of GDC's System is a privilege that may be revoked at any time.

2. Burdensome Use. Users should not perform actions that could excessively burden the resources of GDC's System, such as its data storage capacity or network transmission bandwidth. These actions include, but are not limited to: sending mass mailings or chain letters, spending excessive amounts of time on the Internet for non-business purposes, playing games, uploading or downloading unusually large files, frequent or continuous accessing of streaming audio and/or video files, for non-business related purposes.

3. Unauthorized or Unapproved Software and Devices. Hardware or software which has been obtained from sources outside of GDC, such as disk drives, "thumb drives" and other portable storage media brought from home or received from GDC business partners, may contain computer malware that could damage or impair the performance of GDC's System. Users should never connect outside devices to, or load outside software onto, GDC's System without prior authorization from GDC's Information Technology Department ("GDC IT"). If a User suspects that a virus has been introduced into GDC's System, the User should notify GDC IT immediately.

Users should always exercise extreme care and employ heightened vigilance prior to opening email attachments, or when clicking on embedded links in email received from unknown or suspicious senders.

4. Privacy and System Monitoring. Users are provided access to GDC's System to assist them in the performance of their duties and responsibilities. Users should have no expectation of personal privacy from GDC in anything they create, store, send, receive, use, or access, on GDC's System. Users should assume that any information on or, communications transiting through GDC's System is monitored by GDC personnel or designees.

GDC reserves the right, without notice to any User, to monitor, audit and log any and all aspects of GDC's System and the User's use thereof, including, but not limited to, Internet sites visited by Users, remote access of the system, file uploads and downloads, and communications sent and received by Users. GDC may continue to monitor such communications on GDC's

System (such as e-mails received via the computer network) following the termination of a User's employment.

GDC may utilize software that makes it possible to identify and block access to internet sites containing material deemed by GDC to be inappropriate in the workplace and to monitor computer network and internet usage. Users must never attempt to defeat or circumvent such monitoring or filtering software. If requested, GDC IT may authorize a User access to an otherwise blocked site on a case by case basis.

5. Reporting Instances of Possible Security Issues. Users are required to contact GDC IT immediately upon learning of any of the following potential security issues: (a) loss or theft of any device containing GDC information or used to access GDC's System; (b) possible intrusion into GDC's System; or (c) any suspicious activity that might lead to a security incident on GDC's System. Users are required to cooperate with and to follow instructions of GDC IT or office of the General Counsel of GDC in response to any such report.

6. Compliance with Privacy and Data Control Laws. Users will comply with all applicable privacy and data control laws, rules and regulations. Such laws, rules, and regulations include, without limitation, the US Health Insurance Portability and Accountability Act ("HIPAA") and the European Union's ("EU") General Data Protection Regulation ("GDPR").

B. Prohibited Activities. Users are never, under any circumstance, to perform the following activities on or from GDC's System or from any device remotely connected to GDC's System:

1. Objectionable Content. Without prior written permission from GDC IT, GDC's System may not be used to create, view, store, or transmit: (a) content that violates any of GDC's policies, such as those regarding racist, sexist, pornographic, or other materials that may violate GDC's *Equal Employment Opportunity Policy Prohibiting Discrimination and Harassment*; or (b) any form of computer malware.

2. Copyrighted, Trade Secret and Confidential Information. Users are responsible for complying with copyright, trade secret and other applicable law and applicable licenses or restrictions that may apply to software, files, graphics, documents, messages, information, and other material accessed or transmitted via GDC's System. Users may not agree to a license, download, and install onto GDC's System any material for which a registration, license or other fee is required without first obtaining the express written permission of GDC.

Unless expressly authorized to do so in furtherance of the business of GDC, Users are prohibited from accessing, sending, or otherwise distributing proprietary information, trade secrets or other confidential information that is not the property of the User. Unauthorized access to or dissemination of such information may result in GDC taking severe disciplinary action, including termination, as well as substantial civil and criminal penalties under applicable law.

3. Harmful or Criminal Use. No User may execute any computer program or command with intent to commit or aid the commission of any criminal offense. Unless expressly authorized by GDC IT, a User may not execute any computer program or command with the intent to: (a) interfere with or prevent any other Users access to GDC's System, or any other

computer; (b) breach, circumvent, or disable the security of GDC's System or any other computer; (c) disrupt the operation of GDC's System or any other computer; or (d) damage GDC's System or any other computer.

VI. Access to GDC's System and Information

A. General Access Management. It is the policy of GDC to provide Users access to GDC's System and the information it contains in a manner that fully enables Users to carry out their duties and responsibilities and which is also consistent with GDC's responsibility to safeguard its information and any information entrusted to it. Use of GDC's System is restricted to Users as defined in this policy. Unsupervised use of GDC's System by persons who are not Users as defined by this policy is prohibited. GDC IT manages the means, manner and conditions under which a User may employ a computing device on, or to access remotely, GDC's system and its information.

B. Remote Access Management. Users remotely accessing GDC's System for the purpose of creating, viewing, sorting or transmitting GDC information must do so in full compliance with the provisions of this policy. The use of computing devices to access remotely GDC's System and its information is a privilege which may be suspended or revoked by GDC without prior notification.

Only computing devices which are either (a) owned or provided by GDC IT; or (b) personally owned by a User but equipped with software specified by GDC IT; or (c) preauthorized in writing by GDC IT; will be permitted remote access to GDC information on GDC's System.

C. Passwords. Any desktop, laptop, or mobile computing device owned by or under the exclusive control of a User and which is used to access GDC information on or from GDC's System must be password protected, and also employ a timed log-out feature which, after the initiation of a specified action or the lapse of a selected period of time, automatically restricting access to the computer or device until the User again enters the correct password. Users must never attempt to disengage or circumvent these security protections.

1. System Entry Password. Access to and use of GDC's System requires an authorized User to enter a password into the computing device being used to obtain authorized access to GDC's System. This password must be a complex passcode (i.e., using a combination of letters, numbers, symbols etc.) containing at least eight (8) characters.

2. Remote Device Storage Password. GDC information, stored for any period of time on an authorized computing device outside of GDC's System, requires that access to the device be controlled by a complex passcode containing at least eight (8) characters.

3. Confidentiality. Users must maintain the confidentiality and security of all passwords, keys, or codes used with any computing device accessing GDC's System, or its information. This obligation includes: (a) not selecting easily guessable passwords (such as nicknames, phone numbers, and passwords wholly consisting of publicly available information about the User); (b) disclosing passwords to other persons only on a strict need to know basis; and (c) never displaying usernames or passwords in a conspicuous place or manner.

D. Mobile Computing Devices.

1. Mobile Device Software. Users remotely accessing GDC's System with mobile computing devices must permit the installation of GDC IT-specified mobile device management (MDM) software to enable functions such as (a) monitoring of device system information concerning installed applications, password status, etc.; (b) device password-access control; (c) remote device locking; and (d) remote wiping of GDC information.

2. Device Security. Users agree to take reasonable measures to maintain the security of their mobile computing devices and the information they contain. These measures include: (a) making no effort to circumvent, disable, or defeat the operation of any MDM software installed as required pursuant to this policy; (b) taking no action to "jailbreak", "root" or otherwise modify the normal operations of the device's operating system or of its integrated hardware except solely through and in conformance with the means specifically provide by the manufacturer of the device for this purpose; (c) installing and utilizing the most current device manufacturer-supplied system software and firmware; (d) not allowing unsupervised access to or use of the device by other individuals; and (e) immediately reporting a lost or stolen device to GDC IT. Devices that are reported lost or stolen will be remotely wiped of GDC information and locked. Devices that are subsequently recovered can be unlocked by GDC IT.

3. Device Support. GDC IT technical support for personally owned mobile devices is strictly limited to assisting the User in installing and configuring MDM software and any other GDC selected and required software. Users are personally responsible for all installation, maintenance, servicing, updating, and data backup for their personally owned device, its hardware components, and all software not provided by GDC Users are responsible for all costs and charges incurred by, or associated with, the use and maintenance of the device, whether or not such costs and charges are related to work or personal use. Such charges and costs include, but are not limited to charges resulting from texts, calls, application costs, and telephone carrier fees. Users are responsible for resolving any service or billing disputes with the device carrier.] GDC will provide complete technical support for GDC approved and supplied mobile devices. User may not make modifications of any kind to the hardware or software of GDC supplied devices.

Adopted: September 28, 2018