GovTech Mobile Device Management (Security Suite for Engineering Endpoint Devices – "SEED")
Acceptable Use Policy
(Updated on Jan 2022)

Purpose

This Acceptable Use Policy ("**AUP**") aims to reduce the security risks to the Government managed Device ("**GMD**") and the Government Engineering Resources protected by SEED. The Government Engineering Resources ("**GER**") covers all data, applications and infrastructure used by developers and end users in their course of work in developing Government Applications and Services. The AUP defines standards, procedures, and restrictions for any and all end users ("the **user**") with legitimate business uses connecting devices (equipment or internet device or mobile device) to Government Engineering Resources. Agencies should include their own acceptable use policies to govern the use of their specific resources on top of this AUP. This AUP is in addition to such policies.

The Users may access and use the Services or the Engineering Resources only with a Government Managed Device. The term GMD refers to (A) any equipment or internet device or mobile device that has been furnished by the Government or statutory board (each an "**Agency**"), or (B) any equipment or internet device or mobile device that has been approved for use with the Services by the Government or GovTech through enrolment in GovTech's Mobile Device Management (MDM) services.

All end users using a GMD to connect to GovTech's or the Government's network, and/or capable of backing up, storing, or otherwise accessing data of any type, must adhere to GovTech's processes and policies in doing so.

The AUP may by updated by GovTech from time to time. All end users agree to check the AUP for updates and that such updates are immediately binding whether or not the end user has checked the AUP. GovTech may, at its discretion, notify the end user of any update to the AUP. The updated AUP will be made available at https://docs.developer.tech.gov.sg/docs/security-suite-for-engineering-endpoint-devices/#/.

Applicability

This policy applies to all end users, including full and part-time staff, contractors, freelancers, and other agents who use GMDs to access, store, backup, or relocate any data.

The policy addresses a range of threats to data, or related to its use, such as:

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive data is deliberately stolen and sold by an end user or unauthorized third party.
Malware	Viruses, Trojans, worms, spyware, malware, and other threats could be introduced to or via a mobile device.

Compliance	Loss or theft of data could expose agency to the risk of non-compliance with various laws, rules or regulations.

Addition of new hardware, software, and/or related components to provide additional GMD connectivity will be managed at the sole discretion of GovTech. **Unauthorized use of GMDs to back up, store, and otherwise access any data is strictly forbidden.**

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of devices to any element of the company network and resources.

Affected Technology

Connectivity of all GMDs will be centrally managed by GovTech and will use authentication and strong encryption measures. All end users shall adhere to the same security protocols at all times, **even when connected to non-Agency equipment**. Failure to do so will result in immediate suspension of all network access privileges so as to protect the GovTech's infrastructure.

Policy & Appropriate Use

It is the responsibility of any end users using a GMD to access resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied. GovTech shall also have the right to hold the Agency that granted access to the end user, or for which the end user is using the device for and on behalf of, responsible. It is imperative that any GMD is used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

Access Control

1. GovTech reserves the right to refuse, by physical and non-physical means, the ability to connect GMDs to Government Engineering Resources. GovTech will engage in such action if such equipment is being used in a way that puts its systems, data or users at risk.

2. All GMDs attempting to connect to the Government Engineering Resources through the Internet will be inspected by GovTech. Devices that are not approved, are not in compliance with GovTech's security policies, or represent any threat to the Government Engineering Resources will not be allowed to connect. Devices may only access the Government Engineering Resources through SEED connection.

Mobile Device Management (MDM)

1. GovTech uses the [SEED] mobile device management solution to secure devices and enforce policies remotely. Before connecting a device to any GER, the user shall allow GovTech the rights to install software and collect telemetry from the device and for the device to be manageable by [SEED].

2. [SEED]'s client application must be installed on any devices connecting to GER, including personal devices owned by the end users and devices used by contractors. The application can be installed through the step-by-step guide here. https://docs.developer.tech.gov.sg/docs/security-suite-for-engineering-endpoint-devices/#/

3. The mobile device management solution enables GovTech to take the following actions on GMDs: [remote wipe, remote lock]. **GovTech has the rights to perform any of the actions on the device, even if such device does not belong to a public sector Agency. If a remote wipe action is performed, the end user is to note that ALL data on the device will be wiped and GovTech shall not be liable to the public sector Agency, end user, contractor or such other person owning or having any other rights to the data.**

4. The Users are not allowed to retain or transfer any of the installed software or installation packages to other devices. If there is a need to change device, the user would need to go through the un-enrolment and re-enrolment processes. If the user no longer requires the need to access GER, he/she shall unenroll his/her device.

5. **Any attempt to contravene or bypass the device management implementation will result in immediate disconnection from all Government Engineering Resources,** and there may be additional consequences in accordance with GovTech's overarching security policy, the applicable terms, or at law.

Security

1. The Users using GMDs and related software for network and data access will, without exception, use secure data management procedures. **All GMDs must be protected by a strong password**; a PIN is not sufficient. All data stored on the device must be encrypted using **strong encryption**. End users agree never to disclose their passwords to anyone.

2. The Users of GMDs **must employ reasonable physical security measures**. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.

3. Any non-GovTech computers used to synchronize or backup data on GMDs will have installed **up-to-date anti-malware software required** by GovTech.

4. Passwords and other confidential data, as defined by GovTech, are **not to be stored unencrypted** on GMDs.

5. Any GMD that is being used to store or access GovTech data must **adhere to the authentication requirements** of GovTech.

6. GovTech will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. **Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt** and will be dealt with in accordance with GovTech's overarching security policy, the applicable terms, or at law.

7. **In the event of a lost or stolen GMD, the user is required to report the incident to GovTech immediately. The device will be remotely wiped** of all data and locked to prevent access by anyone other than GovTech. If the device is recovered, it can be submitted to GovTech for re-provisioning. **The remote wipe will destroy all data on the device**, whether or not it is related to GovTech, business or personal.
8. Users must not share accounts. Each user is required to have a unique and identifiable account provisioned.
9. Users shall not delete or disable mandatory applications on the GMDs.

Organizational Protocol

1. GovTech can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the network, and the resulting reports may be used for investigation of possible breaches and/or misuse. **The Agency and end user agree to and accepts that his or her access and/or connection to GovTech's networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. The status of the device, including location, IP address, Serial Number, IMEI, may also be monitored.** This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with GovTech's policies.

2. The end user agrees t**o immediately report** to his/her manager and GovTech **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

Policy Non-Compliance

Failure to comply with the *Mobile Device Management (SEED) Acceptable Use Policy* may result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment or of the relevant vendor contract, by GovTech or the relevant Agency.

By selecting "**ACCEPT**" below it is deemed that you have read, understood and agree to all the provisions in this AUP. This AUP shall apply to you throughout the period that your device is provisioned with SEED and onboarded as a GMD. Any obligations herein that expressly or by their nature survive the cessation of your device as a GMD shall continue to survive.

———————————————————————————————————————