CATALYST
WORKPLACES THAT WORK FOR WOMEN

BRING YOUR OWN DEVICE POLICY

Effective: September 1, 2020

Mobile devices, such as smartphones and tablet computers, are important tools for Catalyst and their use is supported to achieve business goals. However, mobile devices also represent a significant risk to information and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to Catalyst's data and Information Technology (IT) infrastructure. This can subsequently lead to data leakage and system infection. Catalyst is required to protect its information assets to safeguard its customers, intellectual property and reputation. This policy outlines practices and requirements for the safe use of mobile devices.

Purpose of Policy

This policy is intended to protect the security and integrity of Catalyst's data and technology infrastructure. Limited exceptions to the policy may apply due to variations in devices and platforms.

Application of Policy

This policy applies to all mobile and handheld devices, whether owned by Catalyst or by employees, that have access to Catalyst networks, data and systems, including but not limited to, smartphones and tablet computers ("Devices"). This policy does not apply to Catalyst-owned, IT-managed laptops. Employees and contractors are not permitted to use personal computers (desktop or laptop) to perform Catalyst work or access data of a classification higher than Public.

Technical Requirements

- Devices must use a supported Operating System: Android, iOS/iPadOS and Windows 10.
- Devices that are not on Catalyst's list of supported devices are not allowed to access Catalyst's systems.
- Devices must use encryption options for storage, system access and communications.
- Devices must use remote wipe and remote locate features if available.
- Devices are required to have Catalyst-supplied mobile device management (MDM) software installed.
- Devices must lock automatically with a password or PIN if idle for longer than five minutes.
- Devices must automatically restore to defaults after ten failed sign-ins.
- Unless approved by IT, Devices may not connect directly to the internal corporate network.
- Devices must be presented to IT for proper provisioning and configuration, before they may access Catalyst's systems.

User Requirements

- Users must report all lost, stolen or decommissioned Devices to Catalyst's IT department immediately.
- If a user suspects that unauthorized access to company data has taken place via a Device, the user must report the incident immediately.
- Users must not leave unlocked Devices unattended.
- Devices may not be "rooted" or "jailbroken" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
- Users may not load pirated software, unlicensed or illegal content onto their Devices.
- Applications may only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure whether an application is from an approved source, please contact Catalyst's IT department.
- Devices must be kept up to date with manufacturer or network provided software updates and patches. As a minimum, patches should be checked for weekly and applied at least one time per month
- BYOD Device connectivity issues are not supported by IT; users should contact the Device manufacturer or mobile carrier for operating system, hardware or data connectivity issues.
- Devices may not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy.
- Employees and contractors are responsible for not merging personal and work email accounts on their devices. They must ensure that company data is only sent through the Catalyst email system.
- Users may not upload Catalyst data to any cloud storage provider (Box, Dropbox, Google Drive, etc.) or any local storage external to the Device’s mail application.
- Users must not attempt to use Catalyst workstations to backup or synchronize Device content such as media files.

Expectation of Privacy

Catalyst will respect the privacy of the employee’s personal data and will only request access to the Device to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. Catalyst will not use MDM software to access a user’s personal accounts, applications, contacts, email, text or other messages, photos and social networking activity. However, you should have no expectation of privacy with respect to any content created on, transmitted to, received, stored or recorded on the Device in connection with Catalyst business.

Catalyst will not track a user’s location or previous locations when using personally owned devices. When using Catalyst-owned devices, Catalyst will not track a user’s location or previous locations unless attempting to locate a lost or stolen Device or where reasonably necessary to protect Catalyst’s intellectual property or security.

Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee’s personal data from being lost, it is the employee’s responsibility to take additional precautions, such as backing up email, contacts, photos, etc. Catalyst assumes no liability for the loss of personal data. Any use of a Device, whether personal or Catalyst-issued for personal reasons, is done at the employee’s own risk.
- Catalyst reserves the right to disconnect Devices or disable access to Catalyst systems without notification.

- The employee is personally liable for all costs associated with their Device, including monthly subscription fees and additional charges related to data overages and travel.
- Catalyst may remotely delete or “wipe” data from the employee’s Device if necessary, in Catalyst’s judgment, to protect Catalyst interests, including but not limited to if: the Device is lost or stolen, the employee terminates their employment, or IT detects a data or policy breach or a virus or similar threat to the security of Catalyst’s data and technology infrastructure.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of Catalyst and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the Device unusable.

Violations of Policy

- **Non-Compliance.** An employee who violates this Policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

- Data Classification Standard

Definitions and Terms

- **Rooting and Jailbreaking:** The removal of limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

Administration of this Policy

- **Questions.** You are encouraged to ask any questions you may have about this Policy. To learn more, please contact secure@catalyst.org.

- **Reporting.** It is important that you immediately report any suspected violation of this Policy by a Catalyst employee or third party to your manager or to HR. All good faith allegations of violations of this Policy will be fully and confidentially investigated.

- **Exception to Standard.** Limited exceptions to the Policy may apply due to variations in devices and platforms. Management does not have the authority to approve exceptions to this Policy. Any request for an exception to the requirements of this Policy must be submitted to the Information Security Officer, who will review the risk of non-adherence and issue exceptions where deemed prudent.

- **Applicability.** This Policy applies globally unless contrary to local laws and regulations. Operations in different countries may have more stringent policies or implementing procedures where required by local law. In the event of a conflict, these more stringent policies or implementing procedures will take precedence.

Revision History

Date	Name	Description	Responsibility
09/01/2020	James Mbassa	Initial release.	Owner
04/23/2021	James Mbassa	Update regarding location tracking.	Owner