CATALYST
WORKPLACES THAT WORK FOR WOMEN

Acceptable Use Policy

Effective: September 1, 2020

Purpose of Policy

This Policy outlines the use of company technology resources and ensures Catalyst employees clearly understand what is considered acceptable use of company resources.

Application of Policy

This Policy applies to:

1. Company-owned information technology resources, regardless of location.
2. Catalyst employees, contractors and third parties performing services on Catalyst's behalf ("Users") must adhere to this policy. For employees, compliance with this Policy is an expectation of employment (subject to local legal requirements). For contractors and third parties who perform services on Catalyst's behalf, compliance with this Policy is a condition of access to Catalyst facilities and resources, and of being permitted to perform services for Catalyst.

Policy

1. Use of Technology
    a. Catalyst information technology resources (including but not limited to, data, e-mail, Catalyst computing hardware, computer applications, Internet, intranet, facsimile, telephone, voice mail systems mobile phone and other wireless communications devices) ("IT Resources") are company property and are made available in Catalyst's sole discretion for business use.
    b. Users may not perform any personal or non-Catalyst work using Catalyst IT Resources. Incidental personal activities are permitted, as long as the privilege is not abused. Examples of permitted incidental personal activities are making a personal phone call or conducting a personal Internet search that lasts only a few minutes. Catalyst may, in its sole discretion, limit or restrict personal usage of or access to Catalyst IT Resources. Catalyst also reserves the right to remove non-authorized content from Catalyst IT Resources without advance notice.
    c. Users are prohibited from using their company-issued email address, Catalyst network login ID, or Catalyst network password for personal use or to access other online services (e.g., an Amazon, eBay, or a personal banking account).

d. Use of Catalyst IT Resources must comply with company policies and applicable law.

e. Consistent with local laws, Catalyst hereby provides notice that it reserves the right to monitor, record, access, intercept, review, copy, delete, and disclose, in its sole discretion and without further notice, all activities and communications using Catalyst IT Resources. This right extend to any activities considered personal use conducted on or through a Catalyst IT resource, including personal use of the Internet. Use of passwords or other security measures on any Catalyst IT Resource does not diminish Catalyst's right to exercise its rights specified in this Policy.

f. Catalyst reserves the right to wipe, via remote access or otherwise, any Catalyst IT Resource or collect such devices (1) upon termination of employment or service arrangement with Catalyst; or (2) at any time and without notice. PERSONAL INFORMATION SAVED ON A CATALYST IT RESOURCE MAY BE DELETED DURING THE WIPING PROCESS DESCRIBED IN THIS POLICY. You are responsible for backing up your non-Catalyst data separately.

g. Misuse of Catalyst IT Resources will result in denial of future access privileges for third parties, and disciplinary action, up to and including termination of employment, for Catalyst employees.

2. Approved Technologies

   a. Catalyst has issued processes and procedures to define the Standard Technologies (and the major solution components of a technology) for the Catalyst Network, maintain the lifecycle of each Standard Technology, and define how each Standard Technology is used.

   b. Catalyst maintains an inventory of technologies used in the Catalyst Network.

   c. The proposed use of a technology, individually or as part of an architected solution must be reviewed and approved by Catalyst before being purchased, obtained, or otherwise introduced into the Catalyst Network. This must occur prior to hosting/containing/transporting Catalyst data.

3. Removal of Property: IT equipment, and the information stored on it, must be adequately secured when taken off-site, including:

   a. Not displaying Catalyst Internal or Restricted information on laptops or other devices when working in public areas, including on public transport.

   b. When in a car, all equipment and documentation should be locked in the trunk and not on display. Transfer all items into the trunk at the start of the journey so as not to draw attention to the items as the vehicle is left unattended.

   c. When using public transport, items containing Catalyst non-public information should always be within sight.

   d. Due care should be taken with the storage of items at home.

4. Supporter Equipment

    a. Generally, when using Supporter-supplied IT equipment, Users should follow the Supporter's information security policies and procedures. Users should make reasonable efforts to find out which Supporter-specific information security policies and procedures apply to the activities.

    b. Supporter equipment should not be connected to any Catalyst network, except for guest wireless access, unless approved by Catalyst's VP, Information Technology.

    c. Catalyst devices should not be connected to any Supporter network, except for guest wireless access, unless approved by Catalyst's VP, Information Technology and in accordance with the Catalyst Information Security Program.

    d. Any transfer of information from the Supporter to Catalyst should be in accordance with the Information Governance policy and associated procedures.

5. Employee Equipment

    a. No employee personal devices (including memory sticks, cameras, phones, PDAs etc) should be connected to any Catalyst or Supporter IT equipment. The sole exception are mobile devices enrolled in Catalyst's mobile device management solution.

6. Return of Catalyst Property/IT Resources

    a. On or before their last day of employment or upon Catalyst's request at any time, employees must return all Catalyst IT Resources to IT in good working condition as received. This includes, but is not limited to, Confidential Information and all copies thereof, Work Product and all copies thereof, Catalyst documents, manuals, files, keys, credit cards, computers, cell phones, and other equipment.

    b. Employees also are required to delete or destroy all Confidential Information or digital copies thereof, including audio, video, and electronic files, transcribed documents, emailed documents, or any other files containing Confidential Information, that are stored on their computer systems, and certify such deletion to Catalyst.

    c. Employees must assist in transferring back to Catalyst control of any online social media or other accounts they controlled on behalf of Catalyst during their employment.

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

- Bring Your Own Device Policy
- Data Classification Standard

- Information Security Program
- Password Standard

Definitions and Terms

- None

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 Policy.** 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