CATALYST

WORKPLACES THAT WORK FOR WOMEN

INTERNET USE MONITORING AND FILTERING STANDARD

Effective: January 1, 2022

Purpose of Standard

This Standard is intended to define standards for systems that monitor and limit web use from any host within Catalyst's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner and ensure that employee web use can be monitored or researched during an incident.

Application of Standard

This Standard applies to all Catalyst employees, contractors, vendors and agents with a Catalyst-owned or personally owned computer or workstation connected to the Catalyst network.

This Standard applies to all end-user-initiated communications between Catalyst’s network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this Standard.

Technical Requirements

- Web Site Monitoring
    - The Information Technology (IT) Department shall monitor Internet use from all Catalyst-owned computers and devices connected to the corporate network.
    - For all traffic, the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server.
    - Where possible, the system should record the User ID of the person or account initiating the traffic.
        - Internet Use records must be preserved for 60 days.
- Access to Web Site Monitoring Reports
    - General trending and activity reports will be made available to any manager as needed upon request to the IT Department.

  - Incident Response Team (IRT) members may access any and all reports and data, if necessary, to respond to a security incident.
  - Internet use reports that identify specific users, sites, teams, or devices will only be made available to employees outside the IRT upon written or email request to the VP Information Technology from a Human Resources representative.
- Internet Use Filtering System
  - Access shall be blocked to Internet websites and protocols that are deemed inappropriate for Catalyst’s corporate environment.
  - The following categories of websites shall be blocked:
    - Adult/Sexually Explicit Material
    - Advertisements & Pop-Ups
    - Gambling
    - Illegal Drugs
    - File Sharing using unapproved vendors or non-Catalyst email
    - SPAM, Phishing and Fraud
    - Spyware and malware
    - Militancy/Hate and Extremism
    - Violence
    - Weapons/Bombs
    - Illegal activity, hacking or attempts to mask Internet usage
    - Security Risks
- Internet Use Filtering Rule Changes
  - The IT Department shall on an annual basis review web and protocol filtering rules.
  - Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Standard.
- Internet Use Filtering Exceptions
  - If a site is mis-categorized, employees may request a review by submitting a ticket to the IT Help Desk.
    - An IT employee will review the request and un-block the site if it is mis-categorized.

    - Employees may access blocked sites with permission if appropriate and necessary for business purposes.
        - If an employee needs access to an appropriately categorized, blocked, site, the employee's manager will submit a request to Human Resources.
        - HR will present all approved exception requests to the IT Department in writing or by email.
        - IT will unblock that site or category for specific employees, employee groups or the entire organization, based on business need.

Violations of Standard

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

Related Standards, Policies and Processes

- Incident Response Plan

Definitions and Terms

- **Incident Response Team:** In the event of a Security Incident, the CFAO will chair an Incident Response Team (IRT) to investigate, contain and remediate the threat.
- **SPAM:** Electronic junk mail or junk newsgroup postings.
- **Phishing:** The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website.
- **Hacking:** Hacking generally refers to unauthorized intrusion into a computer or a network. The person engaged in hacking activities is known as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.

Administration of this Standard

- **Questions.** You are encouraged to ask any questions you may have about this Standard. To learn more, please contact secure@catalyst.org.
- **Reporting.** It is important that you immediately report any suspected violation of this Standard by a Catalyst employee or third party to your manager or to HR. All good faith allegations of violations of this Standard will be fully and confidentially investigated.
- **Exception to Standard.** Limited exceptions to the Standard may apply due to variations in devices and platforms. Management does not have the authority to approve exceptions to this Standard. Any request for an exception to the requirements of this Standard must be submitted to the Information Security Officer, who will review the risk of non-adherence and issue exceptions where deemed prudent.

- **Applicability.** This Standard 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
12/14/2021	James Mbassa	Policy and URL Category updates.	Owner