CATALYST
WORKPLACES THAT WORK FOR WOMEN

NETWORK SECURITY STANDARD

Effective: September 1, 2020

The Catalyst Information Technology (IT) network consists of an interconnection of networked devices. Catalyst depends heavily upon its IT network and it is essential that the stability, integrity and security of the Catalyst IT network be safeguarded.

Purpose of Standard

This Standard defines the precautions designed to safeguard Catalyst's systems, networks and Catalyst data. When applied, this Standard will reduce the risk associated with the misconfiguration and misuse of network systems and services by specifying the control that shall be present within the network systems.

Application of Standard

This Standard applies to all access to Catalyst's network infrastructure, services and traffic and security services.

Standard

1. Network Administration Roles and Responsibilities: The administration of the Catalyst network infrastructure, including network connections, services, addressing and design, is performed by authorized IT Department staff and its designated agents.
2. Network Segmentation Controls: Controls that permit the passing of approved types of network traffic and specifically disallow or block unapproved traffic shall be in place in the following situations:
    a. Ingress/egress network connections between Catalyst and other networks (e.g., Internet, third-party networks, home user networks).

    b. Between internal network zones (e.g., between corporate and data center networks)

    c. Use of third-party cloud services must be approved by the ISO. All data for which Catalyst is the owner or custodian, and when that data is hosted at a third-party provider, is subject to audit.

    d. Environments hosted at a third-party provider (the "cloud") are subject to the same rules as if they were hosted within the Catalyst network.

3. Encryption: Network traffic shall use an encryption method based on cryptographic techniques that provide strong authentication and security in the following cases:

    a. Traffic consisting of internal data (as outlined in the Data Classification Policy) being transmitted across public networks.

    b. Login credentials passed to network and security devices for administrative purposes.

4. Authentication, authorization and accounting (AAA): AAA must be provided for the following situations:

    a. Administrative and management interfaces of network devices.

    b. Additions and/or changes to the LAN/WAN structure shall be made by an approved agent.

    c. Additions and/or changes to network security infrastructure shall be made by an approved agent.

5. Prevention of misuse:

    a. Controls shall be in place that prevent the use of network systems and services for things other than their intended use or malicious activity.

    b. Network security controls must be implemented to aid in the prevention of misuse of network services, such as proxy abuse, hacking attempts, denial of service attacks, remote compromise of internal systems and defacement or alteration of data.

    c. Non-IT managed equipment, such as Bring Your Own Device (BYOD), customer or partner-owned systems, shall only connect to explicit IT- and security-approved segmented zones, and subject to, where possible, network access controls (NAC) to enforce eligibility for access to a zone based on the user's identity, device type and security posture.

6. Configuration Management: Information systems that process, transmit, or store data shall be configured in accordance with baselines created by expert sources such as Center for Internet Security (CIS), National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

    a. Hardening would typically include removal of unnecessary accounts, disabling or removal of unnecessary services, and enabling security conscious configurations.

    b. Multiple synchronized time sources will be used to retrieve time information on a regular basis so that timestamps in logs are consistent.

    c. All systems that store logs must have adequate storage space for the logs generated.

    d. Before being deployed into production, a system must be certified to meet the applicable configuration standard.

    e. Production devices will be audited periodically to ensure compliance.

7. Monitoring: To ensure that the controls and configurations of network systems and services are enforcing the security standards described in this Standard, the following monitoring systems must be deployed:

    a. Intrusion Monitoring System: An Intrusion Prevention System (IPS) shall be implemented at the network perimeter to detect, analyze and respond to external vulnerabilities and threats.

        i. Thresholds for alarms and alerts shall be configured to identify possible intrusion detection and prevention events or violations of security policies.

        ii. Host-based endpoint management system shall be implemented to detect, analyze and respond to internal vulnerabilities and threats on critical systems.

        iii. Any suspected intrusions, suspicious activity, or system unexplained erratic behavior discovered must be reported to the IT Department.

    b. Network Management System

        i. Use of software or hardware tools on the production network that enables inspection of network traffic, such as packet capturing tools and sniffers, shall be limited to individuals authorized by the IT Department.

        ii. Use of IP scanners, port scanners or any other network scanning tool on the production network is prohibited except for individuals authorized by the IT Department.

        iii. Use of hacking tools, DDOS programs, rogue DHCP servers, or any other software that would be disruptive to the production network is strictly forbidden.

8. Wireless Networking: The IT Department is responsible for providing a secure and reliable network to support the mission of Catalyst. Under this broad responsibility, the following wireless standards apply:

    a. Only Catalyst’s IT Department may deploy and manage wireless access points.

    b. Wireless access points not approved and managed by IT will be removed from the network.

    c. The installation or operation of non-IT-managed (rogue) wireless access points represents a severe security vulnerability and is strictly prohibited.

    d. Unique SSIDs must be used from each wireless access zone (Employees, Guest and Mobile users).

    e. Authentication and encryption is required.

9. Devices may not be connected to more than one network security zone concurrently, with the exception of IT-managed network and security devices.

10. Firewalls: Firewalls must be implemented where the Internet enters the network to mitigate known and ongoing threats.

a. Approval from the ISO is required prior to deploying a new firewall or a change to an existing firewall.

b. Default Deny: All standard firewall deployments will require a “Deny all” rule at the bottom of the configuration.

c. Penetration Testing: Periodic testing of external-facing firewalls is required.

d. Logs: All changes to firewall configurations, services and paths shall be logged.

e. An audit of all network firewall rules must be performed at least annually.

f. Demilitarized Zones (DMZ): All publicly accessible services must be protected by firewalls and be located in a DMZ, a subnet that is protected from the Internet by one or more firewalls.

i. Internal networks shall be protected from the DMZ by one or more firewalls.

ii. Only devices designed for direct inbound Internet access may be placed in the DMZ.

1. Typical production servers should not be connected to the DMZ.

11. Server Connectivity

a. The connection and use of a computer running Server operating system software or otherwise functioning as a server must be authorized by IT.

b. All Servers must have a defined administrator who is responsible for:

i. Server administration and maintenance

ii. Server security, including but not limited to data backup, access control, operating system and application updates and security patches

12. Network Administration

a. In the event of unacceptable network events occurring on the network, IT has the right to gain access to and inspect the configuration of devices or equipment on that network and to request the immediate removal of any devices or equipment that it believes could be the source of the problem.

b. In the event of unacceptable events on a network causing problems on another part of the Catalyst network or on an external network, IT has the right to disable any part of the network as necessary, to remove the source of the problem. While every effort will be made to contact impacted persons, this may not always be possible. All services will be reconnected at the first opportunity.

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

- Log Monitoring Standard
- Patch and Vulnerability Management Standard

Definitions and Terms

- None

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
9/1/2020	James Mbassa	Initial release.	Owner