[Insert Company Name or Logo]	
Title: Network Integrity Protection	**P&P #:**
Approval Date:	**Review: Annual**
Effective Date:	**Security Team**

Purpose
To outline the process for protecting the networks. This includes controlling who can access what network and how data flows across the network.

Scope
This policy applies to all network servers owned or managed by [Company Name].

Policy
Our Security team will implement policies and procedures protecting the integrity of the network through available best practices.

Our workforce members are responsible for complying with our information security network integrity policies and procedures.

Procedures
Our Security team shall implement and monitor a secure network architecture to maintain the integrity of the network.

Workforce members shall be responsible for complying with the established procedures to assist with maintaining the security of the organizations network infrastructure.

Segment Data Processing and Storage Based on Sensitivity
NIST Tier 3 Risk Management Process

1. Group data based on use cases and types of information, and also based on the sensitivity of that data and the level of authority needed to access that type of information.
    a. Once data is segmented, different security parameters and authentication rules should be established depending on the data segment at hand.
    b. The process of segmenting data helps to map out data and determine *who* needs access, *what* they need access to, *when* they need access, and *how* they should be able to access that information.

Use DNS and URL Filtering Services
NIST Tier 3 Risk Management Process

1. Use DNS filtering services on all enterprise assets to block access to know malicious domains.
    a. Block malicious websites
    b. Block phishing websites
2. Consider setting up a blocklist with DNS Filtering

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

3. Set up Uniform Resource Locator (URL) filtering to restrict the websites and content that employees can access.
    a. Enforce safe browsing practices
    b. Avoid malware
    c. Define allow lists

Block Unnecessary File Types
NIST Tier 3 Risk Management Process, Tier 2 Integrated Risk Management Program

1. Implement blocking of unnecessary file types in your security platform
2. Identify specific file types you want to block or monitor
    a. For most traffic (including traffic on your internal network) you will want to block files that are known to carry threats or that have no real use case for upload/download. (Currently, these include batch files, DLLs, Java class files, help files, Windows shortcuts (.lnk), and BitTorrent files.)
3. To provide drive-by download protection, allow download/upload of executables and archive files (.zip and .rar), but force users to acknowledge that they are transferring a file so that they will notice that the browser is attempting to download something they were not aware of.

Establish and Maintain a Secure Network Architecture
NIST Tier 3 Risk Management Process, Tier 2 Integrated Risk Management Program

1. Implement boundary protection devices that employ rule sets or establish configuration settings.
    a. This will assist in enforcing information flow control.
2. Segment the network as appropriate

Perform Traffic Filtering Between Network Segments
NIST Tier 3 Risk Management Process, Tier 2 Integrated Risk Management Program

1. Networks may be segmented for specific reasons thus, filter the traffic between network segments as appropriate.

Violations
Employees who violate these procedures are subject to discipline up to and including termination.

Attachments: None

Related Policies: Workforce Sanction Policy

Reference Sources
- CIS Controls v8 Mapping to NSITCSF final_06-11-2021
- https://www.datamation.com/security/data-segmentation/

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

- https://www.cloudflare.com/learning/access-management/what-is-dns-filtering/
- https://www.fortinet.com/resources/cyberglossary/what-is-url-filtering
- https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/set-up-file-blocking.html

NIST Framework Implementation Tiers

Each subsection of this policy document contains the minimum tier level that correlates with the portion of the policy. The tiers, defined by NIST, are as follows:

Tier 1: Partial,
Tier 2: Risk Informed,
Tier 3: Repeatable, and
Tier 4: Adaptive.

Each tier contains requirements for the categories of Risk Management Process, Integrated Risk Management Program, and External Participation. Some subsections have multiple tiers and categories listed because they meet requirements for different tiers in different categories.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.