System Document	**Kinyo Virginia, Inc.**			
Employee Internet Use Monitoring and Filtering Policy				**Issue: ITP009**
Date: 05/05/2022	**Approved: F. Koshiji**	**Issued By: I.T. Department**	**Revision: 001**	***Page:*** 1 ***of*** 2

1. Purpose

1.1 The purpose of this policy is to define standards for systems that monitor and limit web use from any host within Kinyo network. These standards are design to ensure employees use the Internet in a safe and responsible manner and ensure that employee web use can be monitor or researched during an incident.

2. Scope

2.1 This policy applied to all Kinyo employees, contractors, vendors, and agents with a Kinyo owned or personally owned computer or workstation connected to the Kinyo network.

2.2 This policy applies to all end user-initiated communications between Kinyo network and 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 excluded from this policy.

3. Policy

3.1 Web Site Monitoring

3.1.1 The I.T. department shall monitor Internet use from all 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 are preserved for at least 180 days.

3.2 Access to Web Site Monitoring Reports

3.2.1 General trending and activity reports will be available to any employee as needed upon request to the I.T. Department. Computer Security Incident Response Team (CSIRT) members may access all reports and data if necessary to respond to a security incident with or without an employee submits a Incident Communication Handling Form, (ITF003). Internet Use reports that identify specific users, sites, teams, or devices will only be available to associates outside the CSIRT upon written or email request to Information Systems from a Human Resources Representative.

3.3 Internet Use Filtering System

3.3.1 The I.T. Department shall block access to Internet websites and protocols that are deemed inappropriate for the Kinyo corporate environment. The I.T. department will make exceptions to block list on a case-by-case basis. Some categories have specific sites that are allowed through the filter, such as outlook.com being an exception to the email rule. The following protocols and categories of websites should be blocked.

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging

- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Proxy locations and services
- Social Network Services
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email

3.4 Internet Use Filtering Rule Changes

3.4.1 The I.T. Department shall periodically review and recommend changes to web and protocol filtering rules. H.R. shall review these recommendations and provide any input on any changes that’s made. Changes to web and protocol filtering rules will be record under this policy, “Employee Internet Use Monitoring and Filtering Policy”, (ITP009). The I.T. department can make temporary blocks to any site that shows signs of being infected or compromised or is not correctly labelled or otherwise gets around blocking protocols.

3.5 Internet Use Filtering Exceptions

3.5.1 If a site label is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk by using the Kinyo osTicket Support website (see, WI-IT-008 Os Ticket End User Guide). An I.T. team member will review the request and un-block the site if is mis-categorized.

3.5.2 Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is block and appropriately categorized, they must submit a request to their Human Resources Representative. HR will present all approved exception requests to I.T. department in writing or by email. I.T. will unblock that site or category for that associate only and will track approved exceptions and report on them upon request.

4. Policy Compliance

4.1 **Compliance Measurement:** The I.T. department team will verify compliance to this policy through various methods, including but not limit to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 **Exceptions:** Any exceptions to the policy approved by the I.T. department in advance.