

# **EHLANZENI DISTRICT MUNICIPALITY PROXY FILTERING AND INTERNET ACCESS POLICY FOR 2012**

## **1. OBJECT OF THE POLICY**

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within municipal 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.

### **SCOPE**

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

This policy applies to all end user initiated communications between Ehlanzeni District Municipality'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 policy.

### **POLICY**

#### **Web Site Monitoring**

The ICT Officer shall monitor Internet use from all computers and devices connected to the municipal 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 180 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 ICT Officer. ITC members may access all reports and data if necessary to respond to a security incident through the ICT Officer. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to upper management upon request.

### **Internet Use Filtering System**

The ITC shall block access to Internet websites and protocols that are deemed inappropriate for Ehlanzeni District Municipality's corporate environment. 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
- Social Network Services should be grey-listed in the event of abuse
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate

### **Internet Use Filtering Rule Changes**

The ITC shall periodically review and recommend changes to web and protocol filtering rules. Manual changes to web and protocol filtering rules will be recorded as amendments to this Policy. Changes made automatically by purchased software and subscription services will be available on request.

## **Internet Use Filtering Exceptions**

If a site is mis-categorised, employees may request the site be un-blocked by written request to the ICT Officer. ICT Officer 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 a site that is blocked and appropriately categorized, they must submit a request to the ICT Officer after the Municipal Manager has approved it. All approved exception requests to the ITC Officer must be in writing or by email. The ICT Officer may unblock that site or category for that associate only. The ITC will track approved exceptions and report on them upon request.

### **Disciplinary Action**

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses could violate Ehlanzeni District Municipality's Rules of Order, approved procedure manuals and other work rules, adopted by Ehlanzeni District Municipality from time to time. Ehlanzeni district municipality views violations of this policy in a very serious light and while violations will be assessed on a case-by-case basis, repercussions may vary from a written warning to dismissal or termination of contract(s).

Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of Ehlanzeni District Municipality's resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

### **DEFINITIONS**

#### **Internet Filtering**

Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules.

#### **User ID**

User Name or other identifier used when an associate logs into the corporate network.

**IP Address**

Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.

**SMTP**

Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers.

**Peer to Peer File Sharing**

Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.

**Social Networking Services**

Internet sites such as MySpace and Facebook that allow users to post content, chat, and interact in online communities.

**SPAM**

Unsolicited Internet Email. SPAM sites are websites link to from unsolicited Internet mail messages.

**Phishing**

Attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

**Hacking**

Sites that provide content about breaking or subverting computer security controls.

## **ITC**

Information Technology Committee, with is usually comprised of Upper Management, the ICT Officer and other selected role players.

### **Version Control**

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Details</b>
0.1	23/1/2012	IT	Initial draft.
0.2			
0.3			

## **2. GRIEVANCE AND NON COMPLIANCE**

Should any staff member have a grievance regarding the interpretation or implementation of this policy, such staff member shall abide by the grievance procedure of council as mended from time to time.

Any non compliance by any staff member of this policy, where there are no extenuating or extraordinary circumstances, shall lead to staff members being subjected to discipline in terms of the Council's disciplinary procedure.

## **3. REVIEW AND AMENDMENT OF POLICY**

This policy can be reviewed at any time in full consultation with all staff members, but may only be amended by Council.

## **4. SHORT TITLE AND APPLICATION**

This policy shall be called Proxy Filtering Policy for Ehlanzeni District Municipality and shall come into operation once it is approved by Council.