Company IT Operations & Security Guidelines

1. Email Management

Purpose: Ensure reliable email communication and maintain email security.

1.1 Checking and Sending Emails

- Employees must regularly access company email accounts using:
  - Yahoo Mail
  - Gmail
  - Outlook
- Ensure emails are sent and received correctly. Verify attachments and links before sending.

1.2 Monitoring Spam/Junk

- Regularly monitor the Spam or Junk folders to ensure legitimate emails are not missed.
- Move any legitimate emails from Spam/Junk to Inbox promptly.
- Flag suspicious emails for review.

1.3 Email Authentication

- Verify SPF (Sender Policy Framework) records to prevent spoofed emails.
- Check DKIM (DomainKeys Identified Mail) signatures to ensure the integrity of emails.
- Monitor DMARC (Domain-based Message Authentication, Reporting & Conformance) policies to enforce email security.
- Report any failed authentication attempts to IT immediately.

2. Website Access Control

Purpose: Prevent access to unauthorized or harmful websites and protect company data.

2.1 Blocking Unwanted Websites Using Hosts File

- Open Notepad as Administrator.
- Navigate to C:\Windows\System32\drivers\etc\hosts.
- Add entries to block websites:

  127.0.0.1 www.unwantedwebsite.com
  127.0.0.1 unwantedwebsite.com
- Save changes and flush DNS cache using:

  ipconfig /flushdns
- Verify the blocked sites cannot be accessed.

2.2 Guidelines for Employees

- Access company-approved websites only.
- Do not attempt to bypass restrictions.
- Report any difficulty accessing necessary resources.

3. Reporting & Incident Management

Purpose: Ensure timely response to IT security issues.

3.1 Reporting Suspicious Activity

- Any unusual or suspicious emails must be reported to IT immediately.
- Include screenshots, email headers, or URLs if possible.

3.2 Email Issues

- Report undelivered, delayed, or compromised emails.
- Provide relevant details for IT to troubleshoot effectively.

3.3 Website Access Violations

- Any attempts to access blocked or unauthorized sites should be reported.
- Repeated violations may result in disciplinary action.

Prepared By: [Your Name / IT Department]
Date: [Insert Date]
Version: 1.0