# Acceptable Use Policy (AUP) for [Healthcare Organization Name]

## Introduction

This Acceptable Use Policy (AUP) outlines the standards for acceptable use of computing and information technology resources within [Healthcare Organization Name], which includes three hospitals and 25 clinics. This policy applies to all employees, contractors, and affiliates (hereafter referred to as "users") who access and use these resources. The goal of this policy is to ensure the security, integrity, and reliability of our information technology (IT) resources.

## Scope

This policy covers all IT resources owned or managed by [Healthcare Organization Name], including but not limited to workstations, laptops, mobile devices, network equipment, software, and internet access.

## Policy

1. **Monitoring of User Actions**
   - All user actions on workstations and other IT resources are subject to monitoring by [Healthcare Organization Name]. This includes but is not limited to internet browsing, system login/logout, file access, and application usage.
   - The purpose of monitoring is to ensure compliance with this AUP, safeguard against unauthorized access, and protect the confidentiality, integrity, and availability of patient and organizational data.
   - Users must have no expectation of privacy when using organizational IT resources.
2. **Internet Access**
   - Internet access is provided strictly for purposes directly related to users' roles and job responsibilities.
   - Access to internet resources must be approved by the user's manager and is contingent upon the necessity for such access as determined by job function.
   - Non-essential access to the internet, including but not limited to social media, personal email, and entertainment websites, may be restricted based on the user's role.
3. **Email Usage**
   - Email accounts provided by [Healthcare Organization Name] are to be used exclusively for business-related communication.
   - Limited and reasonable use of email for minimal personal matters is permitted, provided it does not interfere with work duties or compromise the security of the organization.
   - All email communications must comply with organizational policies, including confidentiality and data protection standards.
   - The organization reserves the right to monitor email traffic to ensure compliance with this policy.
4. **Inappropriate Use and Disciplinary Actions**

- Inappropriate use of IT resources includes, but is not limited to, accessing or distributing content that is not related to job responsibilities, engaging in illegal activities, violating confidentiality agreements, and introducing malware into the network.
- Users found in violation of this policy may be subject to disciplinary actions, up to and including termination of employment, legal action, and financial liability for damages caused by the violation.
- Disciplinary actions will be determined based on the severity and frequency of the violations.

**Enforcement**

The IT department is responsible for the enforcement of this policy. Users are required to report any suspected violations or security concerns to their manager or the IT department immediately.

**Acknowledgment**

All users must acknowledge receipt and understanding of this Acceptable Use Policy and agree to abide by its terms as a condition of accessing and using [Healthcare Organization Name]'s IT resources.

**Revision and Review**

This policy is subject to revision as necessary and will be reviewed annually to ensure it remains relevant and effective in managing risks associated with the use of IT resources.

By adhering to this Acceptable Use Policy, users contribute to the security and efficiency of [Healthcare Organization Name]'s operations and the protection of sensitive healthcare information.