**System Monitoring Policy**

**1. POLICY STATEMENT**

[Company Name] reserves the right to monitor individual staff usage in order to guarantee that organizational IT systems are not vulnerable to abuse, but only when permitted by senior HR personnel and where it is fair and acceptable in the circumstances. To guarantee that IT systems are running properly and effectively, a variety of monitoring activities must be created. This covers information entering, leaving, or being stored on an organization's information technology systems. Although such monitoring is not generally person-specific, personal information about employees may be acquired as part of this policy.

**2. PURPOSE**

This policy explains how to keep track of how the system is used and how users interact with it. Its purpose is to assist and inform personnel, as well as to help them realize the need of keeping logs of all system user activity.

**3. SCOPE**

**3.1 IT Assets**

This policy applies to all organizational information systems, as well as employees, contractors, and third-party employees who have access to IT assets and are potentially obligated by contractual commitments.

**3.2 Documentation**

System Monitoring Policy, relevant procedures, and guidelines shall be included in the System Monitoring Policy documents.

**3.3 Document Control**

The System Monitoring Policy document, as well as all other relevant documents, must be kept under strict control. Any document's newest release and preceding version must be preserved using version control. However, for legal and knowledge preservation considerations, the earlier version of the documents will be kept for only two years.

**3.4 Records**

Records created as part of the System Monitoring Policy must be kept for a minimum of two years. Records must be kept in either hard copy or electronic format. The respective system administrators will own the records, which will be audited once a year.

**3.5 Distribution and Maintenance**

All workers covered by the scope of work must have access to the System Monitoring Policy document. All updates and new versions of this document must be made available to the people who need to know. The CISO and system administrators will be in charge of maintaining the System Monitoring Policy document.

**4. Privacy**

The System Monitoring Policy document is to be treated as "confidential" and only given to those who need it with suitable access control. This document's further changes and revisions will be monitored.

**5. Responsibility**

The CISO or selected staff is in charge of ensuring that the System Monitoring Policy is properly implemented.

**6. Policy**

All information security events must be recorded, therefore systems must be monitored. All applicable legal criteria for monitoring and logging activities must be met by the organization. System monitoring will be utilized to verify compliance with the organization's access control and permissible use policies, as well as the effectiveness of the restrictions implemented.

The following features of system monitoring must be considered:

a. regulatory and legislative duties;

b. effective IT system maintenance;

c. prevention or detection of illegal use of, or other threats to, organizational IT systems, or criminal activities;

d. organizational rules and procedures; and

e. review of usage and employee training.

**7. Enforcement**

Any employee who is discovered to have broken this policy may face disciplinary action under the HR Policy.