EMPLOYEE AUP INTERNET USAGE POLICY

[ORGANIZATION LEGAL NAME] Policy Version: 1.0 **Effective Date: Governing Law:** State of [STATE]

---

1. Purpose and Scope

This Acceptable Use Policy (the "Policy") governs the use by Employees (collectively, "Users") of the computer, network, internet, email, and electronic-communications resources (collectively, the "Systems") of **[ORGANIZATION LEGAL NAME]**, a Corporation with its principal place of business at [ORGANIZATION PRINCIPAL ADDRESS] (the "Organization"). By using the Systems, each User agrees to comply with this Policy.

The Systems covered by this Policy include: Computers; Email; Internet; Network.

2. Ownership of Systems

All Systems, including all hardware, software, licenses, network infrastructure, email accounts, user files stored on Organization resources, and data transmitted over the Organization's network, are the **sole property of the Organization**. The Organization retains the right to access, inspect, copy, and delete any data stored on or transmitted through the Systems at any time, with or without notice, subject only to applicable law.

3. Permitted Use

The Systems are provided primarily for Organization business purposes. **Limited, incidental personal use** is permitted provided it (a) does not interfere with the User's duties or the performance of the Systems; (b) does not incur material cost to the Organization; (c) does not violate this Policy or applicable law; and (d) does not create a reasonable expectation of privacy.

4. Prohibited Conduct

Users shall not use the Systems to:

(a) **Violate law.** Engage in conduct that violates federal, state, or local law, including the Computer Fraud and Abuse Act (18 U.S.C. §1030), the Electronic Communications Privacy Act (18 U.S.C. §2510 et seq.), the Stored Communications Act (18 U.S.C. §2701 et seq.), the Digital Millennium Copyright Act (17 U.S.C. §1201 et seq.), or applicable export-control and sanctions laws.

(b) **Harass or discriminate.** Transmit, display, or store content that is discriminatory, harassing, threatening, defamatory, obscene, sexually explicit, or otherwise inappropriate for a professional workplace.

(c) **Infringe intellectual property.** Copy, distribute, or display copyrighted materials, trademarks, trade secrets, or proprietary information without authorization.

(d) **Compromise security.** Attempt to bypass access controls; share credentials; install unauthorized software; disable anti-virus, firewall, or endpoint-security software; introduce malware, spyware, ransomware, or any malicious code; or access accounts, files, or Systems to which the User has not been granted authorization.

(e) **Misuse resources.** Use the Systems for personal commercial activity, solicitations unrelated to the Organization, gambling, illegal downloads, cryptocurrency mining, or excessive streaming or gaming that degrades network performance.

(f) **Breach confidentiality.** Transmit Organization confidential information, trade secrets, personally identifiable information, protected health information, or other sensitive data over unsecured channels or to unauthorized recipients.

5. Anti-Harassment and Anti-Discrimination

The Systems shall not be used to create, transmit, display, download, or store any communication or content that could constitute harassment or discrimination on the basis of race, color, religion, sex (including pregnancy, sexual orientation, and gender identity), national origin, age, disability, genetic information, veteran status, or any other characteristic protected by applicable federal, state, or local law. This Policy supplements, and does not replace, the Organization's separate anti-harassment and equal-opportunity policies.

6. Intellectual Property and Confidential Information

All work product, code, documents, communications, data, and inventions created using the Systems in the course of the User's duties are **"works made for hire"** under 17 U.S.C. §101 and are the exclusive property of the Organization. To the extent any such work does not qualify as a work made for hire, the User hereby assigns all right, title, and interest to the Organization. Users shall not transmit confidential or proprietary information of the Organization or of third parties to personal email accounts, personal cloud storage, or unauthorized recipients.

7. Monitoring and No Expectation of Privacy

NOTICE: ALL ACTIVITY ON THE SYSTEMS IS SUBJECT TO MONITORING AND RECORDING. USERS HAVE NO REASONABLE EXPECTATION OF PRIVACY IN ANY COMMUNICATION, FILE, OR ACTIVITY CONDUCTED ON OR THROUGH THE SYSTEMS.

The Organization conducts routine monitoring of the Systems. Monitoring methods include, without limitation: Email Content; Web Browsing; System Logs.

Records of Systems activity are retained in accordance with the Organization's retention schedule: **90 days for routine logs; longer as required by legal hold or investigation**.

Monitoring is conducted for legitimate business purposes, including: ensuring compliance with this Policy and applicable law; protecting the Organization's confidential information and intellectual property; preventing and detecting security incidents; investigating misconduct; managing network performance; and responding to legal process.

8. Security Responsibilities

Users shall: (a) use strong, unique passwords and enable multi-factor authentication where available; (b) lock or log off devices when unattended; (c) promptly report suspected security incidents, phishing attempts, or lost/stolen devices to the IT Department; (d) not circumvent security controls; and (e) complete required security-awareness training.

9. Enforcement

Violations may result in discipline up to and including termination of employment or contract, revocation of access, and civil or criminal referral where the conduct violates applicable law.

10. Reservation of Rights

The Organization reserves the right to modify this Policy at any time, with or without notice. This Policy does not create a contract of employment and does not alter the at-will nature of any employment relationship.

11. Acknowledgment

By signing below, the User acknowledges that the User has read, understood, and agrees to comply with this Policy, and has received the notices required by applicable law.

User / Employee

_____ PRINTED NAME

_____ SIGNATURE

_____ DATE

**Authorized Representative of **

_____ PRINTED NAME

SIGNATURE

DATE