Data Security: Employee Internet Use Policy

1. **Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment and technology at ABC Company. These rules are in place to protect the employee and the Company. Inappropriate use exposes ABC Company to risks, including virus attacks, compromise of network systems and services, and legal liability.

2. **Scope**

This policy applies to employees, contractors, consultants, temporary employees and other workers at ABC Company, including all personnel affiliated with third parties. This policy applies to all computer equipment and technology that is owned or leased by ABC Company.

3. **Prohibited Uses**

All ABC Company equipment and technology, including, but not limited to, computers, networks, servers and Internet access, are intended for workrelated use only. Employees may not use any ABC Company equipment or technology for personal purposes, including, but not limited to:

1. Downloading, copying, printing or distributing any material that is not related to the employee's job;
2. Visiting websites for reasons unrelated to the employee's job;
3. Downloading, copying, printing or distributing any material that is protected by copyright, trade secret, patent, intellectual property or other laws or regulations, including, but not limited to, installing or distributing "pirated" or other software products that are not appropriately licensed for use by ABC Company;
4. Downloading, printing, copying or distributing pornography, hate material or any material deemed offensive by ABC Company in violation of ABC Company's code of conduct, and discrimination and harassment policies or in violation of relevant laws;
5. Posting or distributing any information about, or lists of, ABC Company's

employees, trade secrets or any other sensitive or confidential information related to ABC Company to parties outside of ABC Company;
6. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws;
7. Introducing malicious programs into ABC Company’s network or servers, including, but not limited to, viruses, worms, Trojan horses, and email bombs; and
8. Effecting security breaches or disruptions of network communications, including, but not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4. **Work Hours**

While in the workplace during work hours, employees are expected to be working, not handling personal matters. Employees must keep their personal interests and activities, including, but not limited to, accessing the Internet for personal reasons, outside of the workplace.

5. **Violations of the Policy**

Employees who violate this policy will be subject to disciplinary measures up to and including dismissal, depending on the circumstances.