Vendor Acceptable Use Agreement

Jefferson County Public Schools

Infrastructure Services
Information Technology
Jefferson County Public Schools

Table of Contents

Executive Summary

Overview

Jefferson County Public Schools (JCPS) supports reasonable access to various electronic information, computer devices and networks for vendors to carry out specific business functions at the school district. Access to computer systems and networks owned or operated by JCPS imposes certain responsibilities and obligations, and access to such is granted subject to JCPS Board policies, and local, state, and federal laws.

Purpose

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at JCPS. This agreement serves to outline the obligations of any vendor who does business with or for the JCPS, or acts as the schools' agent, with regards to provisioning, accessing, or otherwise utilizing JCPS's IT resources. It is the responsibility of every vendor to know these guidelines, and to conduct their activities accordingly.

Scope

All vendors, contractors, consultants, temporary and other non-employee workers at JCPS, including all personnel affiliated with third parties, must adhere to this agreement. This agreement applies to information assets owned or leased by JCPS, or to devices that connect to JCPS network or reside at any JCPS schools or sites.

Policy Statement

General Requirements

- Vendor agrees to develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, security, integrity and availability of all maintained or transmitted JCPS's data.
- Vendor agrees to only use JCPS's data, systems, resources, integrations, and access solely for the original purpose for which it was intended, as stipulated in any contract which exists between Vendor and JCPS.
- Vendor will not mine JCPS's data for any purpose whether internal or external to Vendor Company.
- Vendor will not share JCPS's data with any third party, without express permission of the JCPS authorities in writing.
- Vendor should be aware that the data they create for schools' systems remains the property of JCPS. Because of the need to protect JCPS's network, management cannot guarantee the confidentiality of information stored on any network devices not belonging to JCPS.
- Vendors are responsible for exercising good judgment regarding appropriate use of JCPS resources in accordance with JCPS policies, standards, and guidelines. JCPS resources may not be used for any unlawful or prohibited purpose.
- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Vendor's devices that interfere with other devices or users on the JCPS network may be disconnected.

Vendors Requiring System Accounts

- You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual(s), either deliberately or through failure to secure its access, is a violation of this policy.
- You must maintain system-level and user-level passwords in accordance with the Password Policy.
- You must ensure through legal or technical means that proprietary information remains within the control of JCPS at all times. Conducting JCPS business that results in the storage of proprietary information on personal or non-JCPS controlled environments, including devices maintained by a third party with whom JCPS does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by JCPS, or its partners, for school business.

Vendors Requiring Computing Assets

- You are responsible for ensuring the protection and security of the assigned JCPS assets that includes reasonable protection from any environmental elements. Promptly report any theft of JCPS assets to the immediate supervisor or manager.
- All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, security updates and software distributions such as Windows Update and SCCM.
- Devices that connect to the JCPS network must comply with the Network Use detailed on the next section.

Network Use

You are responsible for the security and appropriate use of JCPS network resources under your control. Using JCPS resources for the following is strictly prohibited:

- Causing a security breach to either JCPS or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.
- Causing a disruption of service to either JCPS or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.
- Introducing honeypots, honey nets, or similar technology on the JCPS network.
- Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.
- Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Use of the Internet or JCPS network that violates the 701 KAR 5:120 that mandates the prevention of sexually explicit materials transmitted to schools via computer.
- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and key loggers.
- Port scanning or security scanning on a production network unless authorized in advance by Information Security.

Electronic Communications

The following are strictly prohibited:

- Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates JCPS policies against harassment or the safeguarding of confidential or proprietary information.
- Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Use of a JCPS e-mail or IP address to engage in conduct that violates JCPS policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a JCPS e-mail or IP address represents JCPS to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

Enforcement

Any violation of this policy may result in termination of services, access, or agreements with the vendor, and be subject to additional actions which may be detailed in the contractual agreement between the vendor and JCPS.

Appendix

Acronyms & Terminologies

Acronym/Terminology	Definitions
honeypot, honey net	Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities.
JCPS	Jefferson County Public Schools
Spam	Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.

References

Descriptions	References
Guidelines for Creating Acceptable Use Policies	http://education.ky.gov/districts/tech/Pages/Acceptable-Use.aspx
Implementation of 1998 Senate Bill230: Acceptable Use Policy and Internet Filtering	http://education.ky.gov/districts/tech/Pages/Senate-Bill.aspx

Version History

Version	Date	Revised By	Reason For Change
0.1	5.31.2016	DL	Draft
1.0	6.14.2016	RS	Final

Document Approvals

Approver Name	Project Role	Signature/Electronic Approval	Date

User Compliance

I have read, understand, and agree to abide by the terms of the JCPS Vendor Acceptable Use Agreement. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

Vendor's Name	Title	Signature/Electronic Approval	Date

Manager(s)/Supervisor(s) Name	Title	Signature/Electronic Approval	Date