Sparta Area Schools

IT Security Administrative Guideline: Vendor & Third-Party Network Access

Effective Date: October 2026

Approved By: Technology Department / Board of Education

Applies To: All Third-Party Vendors, Contractors, Consultants, and External Service Providers

1. Purpose

The purpose of this guideline is to protect Sparta Area Schools' technology infrastructure, internal network integrity, administrative systems, and confidential student/staff data (in compliance with FERPA, COPPA, and Michigan data privacy regulations) from security vulnerabilities associated with unmanaged external hardware.

2. Scope

This guideline applies to all external vendors, contractors, consultants, service providers, software representatives, and technicians working on Sparta Area Schools property or performing services on behalf of the district.

3. Core Guideline Statement

> **Non-District Computers and Unmanaged Hardware Are Strictly Prohibited From Connecting Directly to the Internal District Network.**
>
> Under no circumstances may a vendor, contractor, or external party connect a personal or company-owned laptop, desktop, server, network switch, access point, or other computing device directly into a district Ethernet port (wired LAN) or internal administrative/instructional Wi-Fi network.

4. Approved Network & Device Connectivity Options

Vendors requiring computer or network access while conducting business on Sparta Area Schools property must utilize one of the following approved methods:

Option A: Cellular Hotspot & District VPN Access (For Internal Systems Access)

Sparta Area Schools

IT Security Administrative Guideline: Vendor & Third-Party Network Access

- **Connectivity:** Vendors must provide and utilize their own cellular hotspot (e.g., 5G/4G MiFi or cellular-enabled device) to establish internet connectivity.
- **District System Access:** To access required internal district systems or software applications from an external device, vendors must connect via the district's Virtual Private Network (VPN) through their cellular hotspot connection.
- **VPN Request Process:** Access is not automatic. Vendors needing access to district systems must submit a request using the IT Vendor VPN Access Form. Requests must be approved by both the Sparta Area Schools Technology Department and the Kent ISD Technology Security Team prior to connection setup.

Option B: District-Issued Managed Device

- **Issuance:** If vendor work requires access that cannot be facilitated via VPN or if the vendor lacks cellular connectivity, the vendor must request and use a district-owned, managed device provided by the Sparta Area Schools Technology Department.
- **Compliance:** District devices are pre-configured with required security software, web filtering, enterprise endpoint detection and response (EDR), and active patching.
- **Return of Equipment:** All district-owned hardware must be logged out and returned to the Technology Department upon completion of the contracted work or at the end of each business day, as determined by the IT Department.

5. District Public Wi-Fi Network (Internet Access Only)

Vendors requiring basic internet access while on campus may connect to the district's Public Wi-Fi network without prior IT approval:

- **Network Credentials:**
  - **SSID:** `Public` (or standard public Wi-Fi broadcast)
  - **Password:** `Spartans`
- **Access Scope:** The Public SSID provides **internet access only** and is strictly segregated from all internal district servers, administrative subnets, student databases, and instructional equipment.
- **No Internal Access:** Connecting a non-district device to the Public SSID does **not** grant access to internal network resources, printers, or local administrative systems.

6. Vendor Responsibilities & Compliance

Sparta Area Schools

IT Security Administrative Guideline: Vendor & Third-Party Network Access

- **No Network Tampering:** Vendors shall not disconnect district hardware, bypass network security controls, alter IP settings, or bridge external connections (e.g., bridging a cellular/public Wi-Fi connection with a local wired LAN port).
- **Data Privacy & Confidentiality:** Vendors must adhere to all applicable federal and state data privacy statutes regarding student and staff records.
- **Incident Reporting:** Any suspected security breach, unauthorized access attempt, malware outbreak, or lost/damaged district hardware must be reported immediately to the Sparta Area Schools Technology Department.

7. Enforcement & Penalties

Failure to comply with this guideline poses a direct threat to the cybersecurity and operational continuity of Sparta Area Schools. Non-compliance may result in:

1. Immediate revocation of site access and network privileges.
2. Immediate termination of the underlying vendor contract or service agreement.
3. Financial liability for any remediation, investigation, or recovery costs resulting from unauthorized device connection or subsequent network compromise.

Vendor Acknowledgment & Agreement Form

All vendors performing work on-site at Sparta Area Schools must sign this form prior to beginning work or being granted equipment access.

I have read, understood, and agree to abide by the **Sparta Area Schools IT Vendor Network Access Administrative Guideline**. I acknowledge that non-district owned computers/laptops are not permitted to plug directly into the district's internal network, and I will utilize a self-provided cellular hotspot with an approved district VPN via the IT Vendor VPN Access Form, the district's Public SSID, or a district-provided device as directed.

Vendor Company Name: _____

Representative Name (Printed): _____

Representative Signature: _____ **Date:** _____

District IT Representative Sign-off: _____ **Date:** _____