



Company Guest WiFi and Personal Device Connection Policy

Document ID: DTT-IT-POL-002

Issuing Department: Digital Transformation

Information Classification: For Internal Use Only

Version: 1.0

Issued By: John Lester Rosima - IT Assistant Manager Cybersec/IT Projects

Effective Date: March 30, 2026

1.0 Purpose & Scope

This policy ensures our office stays safe from cyber threats by requiring all personal devices to connect via the **ODVI-GUEST-WIFI** instead of the internal corporate network. Because our security application (**Seqrite**) is only installed on company laptops, we cannot verify the safety of personal phones or tablets. Keeping them on a separate guest connection creates a vital safety barrier that prevents the accidental spread of malware to our internal hardware.

- **Your Personal Devices:** While at the office, your personal phones or tablets must use the Guest WiFi. Once you leave the building, these rules do not apply to your home WiFi or mobile data.
- **Your Company Laptop:** At the office, your laptop must stay on the **Secure Corporate WiFi**. However, when working from home or traveling, you are free to connect to your home WiFi or personal hotspots.
- **Productivity:** This measure does not restrict you; you maintain full access to the internet and tools like Google Drive and Dropbox.



2.0 Roles & Responsibilities

- **Employees & Guests:** Connect personal devices only to the Guest WiFi and follow acceptable use guidelines at all times.
- **IT/Cybersecurity:** Provide access to the Guest WiFi, monitor network traffic, and ensure the Guest WiFi remains isolated from company systems.
- **HR:** Manage policy awareness and oversee disciplinary actions for employees.
- **Governance:** This policy is owned by Digital Transformation/Information Security and supported by HR and Legal, with an annual review to ensure compliance.

3.0 Connection Protocol & Rules

- **Network Name (SSID):** ODVI-GUEST-WIFI.
- **How to Connect:** IT will provide a unique login account or a voucher code.
- **The Rules:**
 - **Allowed:** Use the Guest WiFi for work or personal tasks (email, social media, music, or videos).
 - **Forbidden:** To maintain speed, we limit the Guest WiFi to **10 Mbps** per device. Prohibited acts include bypassing this limit, accessing internal office hardware, sharing passwords with outsiders, or illegal activities like torrenting.

4.0 Security, Privacy & Framework Alignment

To meet global standards (aligned with **NIST Cybersecurity Framework** and **ISO 27001**), we implement the following:

- **Access Control:** We separate personal traffic from company data to protect our "perimeter."
- **Monitoring:** The network is monitored, and connection logs (device IDs and timestamps) are kept for **90 days**. We actively monitor for unusual activities to stop threats before they cause damage.
- **Disclaimer:** Personal devices are used at the owner's risk; the company is not responsible for data loss or malware on personal hardware. Devices sending harmful signals may be removed from the network immediately.



5.0 Policy Violations & Compliance

The IT Team monitors traffic for security. If an unauthorized connection is identified, it will be reported to the employee's Department Head. We focus on coaching first:

1. **First Instance:** A verbal reminder or coaching session to help update your settings.
2. **Repeated Instances:** A formal written warning and a quick security briefing.
3. **Continued Issues:** Disciplinary action as outlined in the Employee Handbook.
4. **Note for Visitors:** For contractors or visitors, repeated violations may result in loss of office internet access.

Prepared by:

John Lester Rosima
Assistant Manager – Cybersecurity & IT
Projects.

Reviewed and approved by:

Michael Singson
Chief of Staff