**Counterfeit Protection Policy**

**10ZiG Technology Inc**

**Effective Date:** 1/1/2025

---

## Introduction

10ZiG Technology Inc is committed to ensuring the authenticity, security, and quality of its Thin and Zero Client Hardware and Software solutions. Counterfeit products can compromise system performance and introduce significant security risks.

This policy outlines how we prevent, identify, and respond to counterfeit or unauthorized products.

---

## Scope

This policy applies to all sales channels including but not limited to:

- End Users
- Authorized Resellers and Distributors
- MSPs and System Integrators

---

## Definition of Counterfeit Products

Counterfeit products include:

- Devices falsely marketed as genuine 10ZiG products
- Unauthorized refurbished or modified devices sold as new
- Hardware containing altered or non-genuine firmware
- Products sold through unauthorized or unverifiable sellers

---

## Prevention Measures

**Authorized Sales Channels**
10ZiG products are sold either through 10ZiG directly or via an approved reseller or distributor. Customers are strongly encouraged to purchase through approved sources.

**Product Authentication**

- Unique serial number assigned to each device
- MAC Address/ID code that can be verified by invoice or by 10ZiG database.
- Secure firmware validation processes

**Supply Chain Integrity**
Strict controls and audits are maintained across manufacturing and distribution.

---

## Identifying Genuine Products

To help ensure authenticity:

- Purchase only from authorized resellers
- Verify serial numbers when available
- Inspect packaging for tampering
- Use official tools to validate firmware

If unsure, contact 10ZiG Technology Inc for verification assistance.

---

## Reporting Suspected Counterfeits

Customers and partners are encouraged to report suspected counterfeit products.

**Report concerns such as:**

- Unusually low pricing
- Missing or altered serial numbers
- Suspicious packaging
- Unexpected device behavior

**Contact:**
Email: support@10zig.com Telephone: 866-865-5250 ext:1

All reports are handled promptly and confidentially.

## Response and Enforcement

When counterfeit activity is identified, 10ZiG Technology Inc will:

- Investigate and document findings
- Take action against unauthorized sellers
- Issue legal notices where appropriate
- Cooperate with law enforcement when necessary

Counterfeit products are not eligible for warranty or technical support.

---

## Security Risks

Counterfeit thin clients may expose organizations to:

- Compromised firmware or hidden backdoors
- Unauthorized network access
- Data security and compliance risks

Any suspected counterfeit device should be removed from use immediately.

---

## Customer Support

For questions about product authenticity or verification, please contact our support team.

---

## Policy Updates

This policy may be updated periodically. The latest version will be available through official 10ZiG Technology Inc directly.