

# Pili International Multimedia Co., Ltd.

## Implementation of Cybersecurity Governance in 2025

### Information Security Risk Management Framework

Under the management center, an Information Department is established to regularly (on a quarterly basis) review information security policies during departmental meetings.

[In accordance with Article 2.24 of the 12th Corporate Governance Evaluation (Year 2025) and the FSC Letter No. 1070210380, the implementation status shall be reported to the Board of Directors.]

#### I. 1/3 Original System Upgrade – NETASK v.9.5

The originally used NETASK v.9.5 served as the core system for the Enterprise Information Portal and had been operating stably for many years. However, with the expansion of business needs, rising expectations for user interface design, and updates to information security standards, the original version gradually became insufficient to meet modern management requirements.

##### Upgrade Objectives:

- Enhance system performance and stability
- Improve user experience (UX/UI)
- Expand module functionality and integration
- Comply with the latest information security standards (e.g., ISO 27001, GDPR)
- Support mobile devices and cloud architecture

#### II. Apex One Console Upgrade Plan (August 15–22)

To enhance cybersecurity protection and system stability, the Information Department will carry out a phased upgrade of the Trend Micro Apex One console version.

##### Upgrade Objectives:

- Strengthen malware detection and protection capabilities
- Improve console performance and user experience
- Fix known issues and security vulnerabilities in the current version
- Comply with the latest cybersecurity policies and regulatory requirements

#### III. Upgrade Schedule and Version Details

Date	Upgrade Phase	Post-upgrade Version	Description
August 15 (Fri)	Phase 1 Upgrade	11564	Core console module update, including management interface optimization and partial protection module enhancements
August 22 (Fri)	Phase 2 Upgrade	14081	Full upgrade to the latest version, covering advanced threat protection technologies and enhanced Endpoint Detection and Response (EDR) capabilities

IV. **Cybersecurity Awareness Message :**

**Beware of Fake Tax Audit Emails Targeting Taiwanese Enterprises!**

A hacker group is impersonating the National Taxation Bureau and distributing malicious software known as **Winos 4.0** through fraudulent emails claiming to conduct random tax inspections.

- V. As of October 2025, there have been **no major cyberattacks or data breaches** affecting the company's information security or business operations.

VI. **Cybersecurity-Related Training (January to October, 2025) :**

Date	course	Man*hours
2025/3/04	Explanation of Cybersecurity Incidents and Preventive Measures (E-Course)	8
2025/3/20	Guidelines for Information and Communication Security Controls (E-Course)	
2025/2/26	Cybersecurity Awareness, Essential Knowledge and Responsibilities (E-Course)	4
2025/5/05	AI Development and Cybersecurity Risks	3
2025/6/13	Leading Strategies for Enterprises in AI Transformation	3

【Implementation Status Data Source: Information and Technology Department, Human Resources Department】