

- Translation -

Definitions

Company / Organization	refer to	Asset Five Group Public Company Limited.
Subsidiary	refer to	Any company or legal entity in which Asset Five Group Public Company Limited holds, directly or indirectly, more than fifty percent (50%) of the voting rights.
Asset Five Group or the Group	refer to	1. Asset Five Group Public Company Limited; and 2. its subsidiaries.
The Board of Directors	refer to	The directors of Asset Five Group Public Company Limited.
Executives	refer to	The Chief Executive Officer (CEO) and the next four highest-ranking executives following the CEO, including all persons holding equivalent positions to the fourth-ranking executive, as well as executives in accounting or finance functions at the level of department head or higher, or equivalent.
Remote Desktop	refer to	A technology that enables users to remotely access and control a computer or server through the internet or a local area network (LAN). This allows users to operate another computer as if they were physically present in front of that computer, even when they are in a different location.
IP Address	refer to	An address used to identify and connect devices connected to the internet or a local area network, indicating the source or destination of data transmitted over the network.

VPN	refer to	A Virtual Private Network (VPN), a technology that enables users to establish a secure connection between their devices, such as computers or smartphones, and the internet or an organization's network through an encrypted connection, thereby helping protect data from interception or attacks by third parties.
Log	refer to	A record of events or activities occurring within a computer system, server, or application, which is used to track, monitor, and analyze system operations, particularly when problems or errors occur.

Objectives

This Policy is established to define the rules and guidelines for controlling the use of Remote Desktop within the organization, in order to ensure that remote connections and access to information are conducted securely and efficiently, in compliance with personal data protection laws and the Company's information security requirements.

Scope

This Policy applies to all use of Remote Desktop software, including remote access to servers by external service providers that have service agreements with the Company for system troubleshooting, maintenance, and software upgrades, using programs or tools that support remote access (Remote Desktop).

1. Request for Remote Desktop Access

1.1 An employee who receives a request to use Remote Desktop shall submit an approval request by e-mail to the Information Technology Officer, specifying the requester's full name, the software to be used, the purpose and scope of access, and the approximate time at which the requester intends to remotely access the user's computer.

1.2 The Information Technology Officer shall review the request as follows:

- **Approved:** Approval may be granted where, based on the stated purpose and scope, the requested remote access does not adversely affect information security. The Information Technology Officer shall monitor the requester's activities throughout the remote access session and, upon completion, verify that the connection between the employee's computer and the requester has been terminated.

- **Not Approved:** Approval shall not be granted where, based on the stated purpose and scope, the requested remote access may adversely affect information security, such as where access to certain confidential Company information is required.

2. Security Requirements

2.1 Prior to using Remote Desktop, the employee shall log out of any unrelated systems and close all unrelated information. During a Remote Desktop session, if the employee or the Information Technology Officer identifies any activity that is inconsistent with the approved purpose and scope, the connection shall be immediately terminated, and the requester's organization shall be notified for further investigation.

2.2 Employees who are not based at the Head Office shall connect through the VPN whenever accessing the internet in order to protect data from interception by unauthorized or malicious persons.

2.3 Employees shall access only the information and systems necessary for the performance of their duties. Access rights shall be assigned according to their designated roles and responsibilities.

2.4 All connections and significant activities shall be recorded in system Logs and shall be retained and available for retrospective review for 90 days, in accordance with applicable legal requirements.

2.5 Where the Information Technology Officer needs to use Remote Desktop to access an employee's computer for preliminary inspection and troubleshooting, the employee shall be notified in advance via e-mail or Google Chat, in accordance with the Company's internal communication policy.

3. Prohibited Use of Remote Desktop

3.1 Remote Desktop shall not be used for any activities unrelated to work or for personal purposes.

3.2 Remote Desktop shall not be used to connect with other persons within the organization unless necessary. Where such access is required, an approval request shall be submitted by e-mail to the Information Technology Department in advance, in the same manner as remote access involving external parties, in order to prevent data leakage.

Policy Review

The Company shall review the Remote Desktop Policy of the Company and its subsidiaries at least once a year, or whenever there is a significant change in risk factors affecting the business of the Company and its subsidiaries.

This Remote Desktop Policy was revised for the first time and reviewed at the Board of Directors' Meeting No. 5/2025, held on 12 November 2025, and shall be effective from 12 November 2025 onwards.

Announced on 12 November 2025

-Manop Bongsadadt-

(Associate Professor Manop Bongsadadt)

Chairman of the Board of Directors

Asset Five Group Public Company Limited