NetGain systems	No of Pages	**1** of **4**
	Document Classification:	Internal
	Effective Date	1 Aug 2025
GUIDELINES FOR REMOTE WORKING	Doc No	ISMS-PPL-04
	Revision	1.0

AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Bint Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

THIS DOCUMENT IS ELECTRONICALLY CONTROLLED.
PRINTOUTS OF THIS DOCUMENT MAY BE OUT OF DATE AND SHOULD BE CONSIDERED UNCONTROLLED.

TABLE OF CONTENTS

PURPOSE

This procedure sets out the information security measures to be implemented when personnel are working remotely to protect information accessed, processed, or stored outside the organisation's premises.

SCOPE

This control applies to all employees granted privileges to work remotely.

REFERENCE

ISO/IEC 27001 Standard	Annex A 6.7 Remote working

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

The Management Representative is responsible to ensure that this control is implemented and personnel working remotely are complying with the information security measures stated herein.

PROCEDURE

1. Guidelines

Employees are only permitted to work remotely if approved for a remote work arrangement and with permission from their immediate superior or if an organisation mandate has been put in place. The nature of the employee's work and responsibilities must be conducive to a flexible work arrangement without causing significant disruption to performance and/or service delivery.

Remote work privileges do not change the conditions of employment or required compliance with policies. It is the employee's responsibility to ensure that information is not put at risk in remote work arrangements.

2. Equipment

Any equipment issued used by the remote worker must be configured with the standard security settings in line with *ISMS-TECH-01 User Endpoint Devices.* The remote worker shall acknowledge and comply with the organisation's policies and rules for acceptable use. The remote worker is financially responsible for any intentional damage to equipment, and loss or damage resulting from gross negligence by the employee.

Specifically, the remote worker must:

- Keep their equipment password protected.
- Store equipment in a safe and clean space when not in use.
- Lock the screen when unattended.
- Follow all data encryption or password protection standards and settings.
- Refrain from downloading suspicious, unauthorized or illegal software.
- Not bypass any security configurations set up in the device e.g., anti-virus, firewall.
- Store files in designated company drives / folders to ensure consistent back-up.
- Update operating systems timely.

3. Remote Access

To ensure that no risk is placed on the organisation’s information systems in implementing remote access, the following will be ensured:

- Any remote access should be performed over encrypted channels.
- Technologies such as device attestation, certificate-based authentication, multi-factor authentication and conditional access policies to be considered for enhanced security.
- For VPN connectivity, only company approved VPN client can be used and a list of VPN users shall be maintained by IT.
- Other considerations must be followed in line with *ISMS-ORG-07 Access Control.*