



ITMS POLICY · WORK FROM HOME

Work From Home Policy Adherence

How every NTPL employee working remotely protects company assets, keeps data secure and represents us professionally to our clients.



DOCUMENT NO.
NTPL-ITMS-POL-WFH-01

VERSION
1.0

EFFECTIVE DATE
10 October 2026

CLASSIFICATION
Internal

Working remotely, securely.

Working from home gives us flexibility, but it also moves company equipment, company data and client conversations outside the protection of our office. This policy, part of NTPL's IT Management System (ITMS), sets out what every employee must do to keep those safe while working remotely.



Purpose

To define clear, practical rules for the use of NTPL IT assets, information and communication channels when employees work from home or any other remote location.



Who it applies to

All permanent and contract employees, trainees and consultants who are approved to work remotely, full time or part time, and who use any NTPL asset, account or client data.

Our six commitments at a glance



Safe workspace

A private, secure place to work with a protected home network.



Asset care

Company equipment is used, stored and transported with care.



Data security

Data stays on approved, encrypted, company systems only.



Access control

Strong passwords, MFA, and no shared accounts, ever.



Client trust

Professional, confidential conduct with every client.



Report fast

Any loss, damage or incident is reported immediately.

Contents

#	Section	Page
01	Home workspace & secure connectivity	3
02	Care of company assets	4
03	Data security & access control	5
04	Incident reporting & threat awareness	6
05	Client handling & professional conduct	7
06	Monitoring, compliance & daily checklist	8
07	Employee acceptance & declaration	9

SECTION 01

Home Workspace & Secure Connectivity

Your home becomes an extension of our office. Set it up so that company work stays private and protected.



Your workspace

- ✓ Work from a **quiet, private area** where screens and calls cannot be seen or overheard by family members, visitors or neighbours.
- ✓ Position your screen **away from windows and doorways**; use a privacy filter where provided.
- ✓ Keep a tidy desk. **No printed client or company documents** are left in shared areas; store them in a lockable drawer and shred them when no longer needed.
- ✓ Do not work on company data from **cafés, co-working spaces or public transport** unless your manager has approved it and you are on the company VPN.

Secure home network

- ✓ Use **WPA2 or WPA3** encryption on your Wi-Fi. Never use open or WEP networks.
- ✓ Change the router's **default admin password** and Wi-Fi password to strong, unique values.
- ✓ Keep router firmware **updated**; restart it at least once a month.
- ✓ Connect to the **company VPN** before accessing any internal system, file share or client environment.
- ✓ Never connect company devices to **public or unknown Wi-Fi**; use your mobile hotspot instead.
- ✓ Disable Bluetooth and file sharing when not in use.

Availability & working hours

Requirement	Expectation
Working hours	Follow your approved shift. Be reachable on company chat, email and phone during these hours.
Internet connectivity	Maintain a stable connection suitable for video calls; keep a backup (mobile hotspot) ready.
Power backup	Keep the laptop charged; inform your manager promptly of outages that affect work.
Attendance	Mark attendance and log time in the company's approved tools only.



Remember: the company VPN, antivirus and endpoint agents installed on your device must stay on at all times. Disabling, uninstalling or bypassing them is a policy violation.

SECTION 02

Care of Company Assets

Every laptop, accessory and device issued to you is registered in the NTPL ITMS asset register and remains company property.



Issue, ownership & tracking

- ✓ Assets are issued against your name and **asset tag** in the ITMS register. Check the tag, serial number and condition on receipt and report any mismatch within **24 hours**.
- ✓ Company assets are for **official work only**. They must not be used by family members, friends or anyone else, or for personal business.
- ✓ Do not remove asset tags, open the device or swap parts. Repairs are handled **only by NTPL IT** or its authorised vendor.
- ✓ Allow the IT team's inventory and monitoring agents to run; they keep the asset register, installed software list and warranty records accurate.

Do

- ✓ Use a padded bag when travelling; keep it with you at all times.
- ✓ Keep devices away from water, heat, direct sunlight and food.
- ✓ Use a surge protector and the original charger.
- ✓ Shut down or lock (Win + L) the device whenever you step away.
- ✓ Store devices out of sight and out of reach of children and pets.

Don't

- ✗ Leave devices unattended in a vehicle, café or public place.
- ✗ Lend, sell, pledge or hand the asset to anyone else.
- ✗ Attach personal USB drives, phones or unknown peripherals.
- ✗ Install pirated, cracked or unlicensed software.
- ✗ Disable antivirus, firewall, encryption or the VPN client.

Loss, theft or damage

Situation	Report within	What you must do
Theft or loss	Immediately	Inform IT and your manager so the device can be locked and wiped remotely; file a police report (FIR) and share a copy.
Physical damage	Within 24 hours	Stop using the device if unsafe; raise a ticket with photos. Repairs follow the AMC or warranty process.
Malfunction	Same working day	Raise a helpdesk ticket; do not attempt repairs yourself.
Exit or transfer	Last working day	Return all assets, chargers and accessories in good condition; IT signs the return in the ITMS register.

Loss or damage caused by negligence or misuse may be **recovered from the employee** as per company HR policy.



Data Security & Access Control

Company and client information is our most valuable asset. Protect it as if it were your own.



Device security

- ✓ Full-disk **encryption** (BitLocker or equivalent) stays enabled.
- ✓ Screen **auto-locks within 5 minutes**; lock manually every time you leave.
- ✓ OS, browser and antivirus updates are installed **without delay**.
- ✓ Only **IT-approved software** is installed; request anything else through the helpdesk.



Passwords & access

- ✓ Use strong passphrases of **12+ characters**, unique for each system.
- ✓ **Multi-factor authentication** and email login codes are mandatory where available.
- ✓ Never share passwords, OTPs or login codes, not even with IT or your manager.
- ✓ Do not save company passwords in personal browsers or notebooks.



Handling information

- ✓ Store work files only on **company-approved storage** (company drive, email, approved cloud). Never on personal laptops, phones, USB drives or personal cloud accounts.
- ✓ Never forward company or client data to **personal email** or messaging apps such as personal WhatsApp or Telegram.
- ✓ Avoid printing at home. If printing is unavoidable, collect it immediately and **shred** it after use.
- ✓ Do not paste company or client data into **unapproved AI tools**, translators or online converters.



Information classification

Class	Examples	How to handle when working from home
Public	Website content, brochures, published offers	May be shared freely.
Internal	Policies, internal emails, process documents	Company systems only; not shared outside NTPL.
Confidential	Client data, network diagrams, IP plans, pricing, contracts	Need-to-know access; encrypted transfer; never printed or stored locally.
Restricted	Passwords, credentials, personal data, financial records	Only in approved vaults or systems; never emailed, screenshotted or written down.

SECTION 04

Incident Reporting & Threat Awareness

Attackers target remote workers. Spot the signs early and report quickly; speed limits the damage.



Recognise the warning signs

Phishing emails

Urgent requests, unknown senders, look-alike domains, unexpected attachments or links asking you to log in.

Fake calls & messages

Callers posing as IT, a manager or a client asking for OTPs, passwords or remote access to your device.

Device symptoms

Pop-ups, sudden slowness, unknown programs, disabled antivirus or files you did not change.

What counts as a security incident

- ✓ Lost or stolen laptop, phone, token or ID card
- ✓ Clicking a suspicious link or opening a malicious attachment
- ✓ Sharing a password or OTP by mistake
- ✓ Sending data to the wrong person or client
- ✓ Unknown login alerts or MFA prompts you did not start
- ✓ Anyone viewing confidential data without authorisation

Incident response: your five steps



1 Stop

Don't click further, don't delete evidence.

2 Disconnect

Turn off Wi-Fi or unplug network if malware is suspected.

3 Report within 1 hour

Inform the IT helpdesk and your manager.

4 Cooperate

Follow IT instructions; share screenshots and details.

5 Close

IT confirms resolution and records lessons learned.

IT helpdesk contacts



EMAIL

support@namisite.com

PHONE / WHATSAPP

+91-926-797-1645

TICKET PORTAL

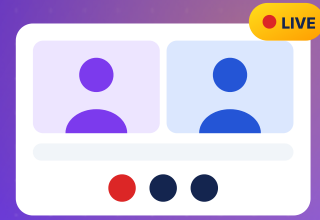
helpdesk.namisite.com



No blame for reporting. Employees who report an honest mistake promptly will be supported. Hiding or delaying an incident is a serious violation.

Client Handling & Professional Conduct

Every call, email and message you send from home represents NTPL to our clients.



Communication

- ✓ Use only **official channels**: company email, approved meeting tools and company phone numbers.
- ✓ Respond to client queries within agreed **SLA timelines**; set an out-of-office when unavailable.
- ✓ Keep written communication clear, polite and accurate. Copy your manager on commitments.
- ✓ Never share your **personal number** or personal social profiles for client work.



Video calls

- ✓ Dress **professionally**; use a neutral or company-provided virtual background.
- ✓ Join from a quiet place; **mute** when not speaking and use a headset.
- ✓ Before **sharing your screen**, close unrelated windows, chats and other clients' data.
- ✓ Record meetings only with the **client's consent** and store recordings on company systems.



Client confidentiality

- ✓ Honour every **NDA and contract** signed with the client. Client information is used only for that client's work.
- ✓ Access client networks, servers and portals only through **approved remote-access tools** and only for authorised tasks.
- ✓ Never discuss one client's systems, issues or pricing with another client, or on social media.
- ✓ Client credentials, network diagrams and IP details are **Restricted** and must stay inside approved systems.



Escalation & complaints



If a client asks you to work outside agreed scope, share data through an unapproved channel, or bypass a security control, **politely decline and inform your manager**.

SECTION 06

Monitoring, Compliance & Daily Checklist

Simple habits, done every day, keep you and NTPL compliant.



Monitoring

To protect company and client data, NTPL may monitor the use of company devices, accounts and networks. This includes:

- ✓ Asset inventory, installed software and patch status
- ✓ Network and VPN connection logs
- ✓ Email and system access logs
- ✓ Antivirus and security alerts

Monitoring is limited to company assets and accounts and is carried out in line with applicable law.

Non-compliance

Breaches of this policy will be reviewed by IT, HR and management. Depending on severity, consequences may include:

- ✓ Re-training and a written warning
- ✓ Withdrawal of work-from-home approval
- ✓ Recovery of cost for lost or damaged assets
- ✓ Disciplinary action up to termination, and legal action where the law is broken

My daily WFH security checklist

START OF DAY

- ☐ Private workspace, screen not visible to others
- ☐ Connected to secure Wi-Fi and company VPN
- ☐ Antivirus active, pending updates installed
- ☐ Logged in with MFA; no shared accounts

DURING THE DAY

- ☐ Lock screen whenever I step away
- ☐ Files saved only on approved storage
- ☐ Checked links and senders before clicking
- ☐ Client calls professional and on official tools

END OF DAY

- ☐ Disconnected VPN, shut down device
- ☐ Printed papers locked away or shredded
- ☐ Device stored safely, out of reach
- ☐ Any issue reported to IT helpdesk

Policy review

This policy is owned by the NTPL IT department and reviewed at least once a year, or sooner when technology, law or business needs change. Employees will be informed of every revision and may be asked to re-accept it.

Employee Acceptance & Declaration

Please read, complete and sign. Return the signed copy to HR. A copy is kept with your ITMS asset record.



Declaration

I, the undersigned, confirm that I have received, read and understood the **NTPL Work From Home ITMS Policy (NTPL-ITMS-POL-WFH-01, v1.0)**. I agree to comply with it at all times while working remotely. In particular, I confirm that:

- ☐ I will take full care of the company assets issued to me and return them on request or on exit.
- ☐ I will keep company and client data confidential and only on approved systems.
- ☐ I will handle clients professionally and only through official channels.
- ☐ I will report any loss, damage or security incident immediately.

I understand that NTPL may monitor company assets and accounts, and that non-compliance may lead to disciplinary action and recovery of losses.

Employee details

EMPLOYEE FULL NAME

EMPLOYEE ID

DEPARTMENT

DESIGNATION

REPORTING MANAGER

CONTACT NUMBER

COMPANY ASSETS ISSUED FOR WORK FROM HOME

Asset tag

Asset type / model

Serial number

EMPLOYEE SIGNATURE

DATE

SIGN HERE

/ /

PLACE

FOR OFFICE
USE

VERIFIED BY (HR / IT)

SIGNATURE

DATE

