	Information Security Management System	<b>Document Title:</b> Working from Home Policy		<b>Document Ref:</b> POL 032
		<b>Issue No.</b> 2	<b>Date:</b> Nov 23	<b>Page No:</b> 1 of 2
	<b>Classification:</b> Internal use only			

## 1 Purpose

Globalization Partners (G-P) allows employees to work from home under the G-P Remote First Policy and provides the required infrastructure to work remotely efficiently. The purpose of this policy is to outline guidelines and eligibility criteria for working from home.

## 2 Scope

This policy applies to all employees and contractors at G-P. It does not change or replace the terms and conditions of employment or the need to comply with existing company policies, rules, and practices.

## 3 Policy

### 3.1 General Requirements

- All employees working from home shall obtain approval from their supervisor.
- All employees working from home shall comply with G-P's existing policies.
- Employees shall be available and accessible to their supervisor and co-workers during the agreed work hours and notify their supervisor in the event of any emergency, including illness, injury, power failure or loss of internet connectivity.

### 3.2 Equipment and Tools

G-P shall provide employees authorized to work from home with the resources necessary to perform their duties, including laptops and peripheral devices. The use of equipment belonging to G-P is for use only by the designated persons and for organization-related purposes.

Maintenance and repair of personally owned equipment are the responsibility of the employee. All personally owned equipment, such as computer hardware and software, must meet G-P's configuration and security requirements stated in G-P's security policies.


### 3.3 Data Security

When working from home, G-P's employees shall abide by the G-P's security policies to ensure data protection, confidentiality and security, including:

- Securely destroying any printed confidential and business documents that are not required to be retained.
- Storing any printed business documentation in a locked and secure place.
- Not permitting access to G-P's resources or any G-P documents to any third party, including family members.
- Remotely accessing G-P's resources following guidelines approved by the IT department.

### 3.4 Home Wireless Device Requirements

G-P prescribes these best practices for wireless infrastructure devices that provide direct access to the G-P corporate network:

	Information Security Management System	<b>Document Title:</b> Working from Home Policy		<b>Document Ref:</b> POL 032
		<b>Issue No.</b> 2	<b>Date:</b> Nov 23	<b>Page No:</b> 2 of 2
	<b>Classification:</b> Internal use only			

- Ensure that the home network is configured properly and hardened.
- Change all default passwords on the wireless infrastructure devices and use strong, complex passwords.
- Ensure home wireless routers are configured to use WPA2 or WPA3 wireless encryption standards at the minimum and disable legacy protocols such as WEP and WPA.
- Ensure the wireless network name (service set identifier [SSID]) does not identify physical location or router manufacturer/model.
- Ensure the router firmware is updated where applicable.
- Printers should be connected directly to G-P owned laptops via USB or other secure direct connections. Any use of wireless protocols in print devices should be avoided whenever possible. Use of printers for printing any materials should be limited to work-related files exclusively. Access to printing is restricted through G-P's device control program. If you need access to print files, please open a ticket with IT department.
- Printing should be avoided from home offices unless absolutely necessary. Any printed documents requiring signatures should be scanned and saved in appropriate G-P document libraries, and the printed document destroyed or shredded.

## 4 Change history

Issue	Date	Details
1	01 Aug 2022	Created
	04 Nov 2022	Reviewed and revised – Jim Barr
	08 Nov 2022	Approved – Mike Gross
2	01 Nov 2023	Reviewed and revised – Maria Lees
	05 Nov 2023	Approved – Leila Pourhashemi