Purpose

The purpose of this policy is to:

- defines the roles and responsibilities of relevant persons.
- provide a safe and secure working environment and promote the protection of assets.
- to protect service users, staff and visitors.
- to identify sensitive areas within the organisation.
- to define and restrict access to the same.

Maintain the security of confidential information (such as “Company” sensitive information and personal identifiable information (“PII”), as well as the information shared with GOAL by its service users and partners. GOAL strives to maintain service user friendly procedures to ensure only authorised employees, contractors, and visitors have access to its facilities.

Scope

This policy applies to all employees, contractual employees, self-employed employees, trainees, volunteers and all other visitors.

This policy applies to the physical areas occupied by Go-Woman! Alliance on these sites, where information assets are kept. These areas include office areas that maintain Company Sensitive Information or PPI. These areas must be physically secured to prevent theft, tampering or tapping, or damage.

Responsibility

GOAL designated personnel are responsible for proper implementation of the Physical Security Policy.

Policy

Following are the policies defined for maintaining Physical Security:

1. Access to the dropbox shall be restricted only to designated personnel and password protected.
2. All physical access points (including designated entry / exit points) to the facilities where information systems reside shall be controlled and access shall be granted to individuals after verification of access authorization.
3. Access to the building (locked door)is monitored and controlled via reception (office manager). Where a risk has been highlighted additional measures of control will be implemented.
4. The access records of the visitors shall be maintained.
5. Visitors shall be escorted by the designated personnel and their activities, if required, shall be monitored.
6. Systems Personnel shall examine laptops of visitors for latest anti-virus definition, latest patches and updates, and any sort of vulnerability which could be harmful for the network.
7. Any user who needs to connect to external network for official work shall be able to do so after an official sanction from Management and Security Team. This team shall evaluate security risks before issue of any sanction.
8. A record of all physical accesses by both visitors and authorized individuals shall be maintained.
9. All policies stated above shall be monitored for any changes from time to time.

It is every employee's responsibility to work towards, maintaining and preserving a secure physical work environment.

Policy Review

This policy will be reviewed annually, or as new knowledge on the subject evolves and subsequent guidance is issued.

Reviewed: 5th September 2025 Review date: September 2026