GWS

GWS Information Security Policy

GWS-ISI-001 · Version 1.0

Institutional Use Issued 09/03/2026

CONTENTS

00

DOCUMENT CONTROL

Field	Value
Code	GWS-ISI-001
Version	1.0
Issued	09/03/2026
Revised	09/03/2026
Approved by	GWS Management
Owner	Institutional Governance
Classification	Institutional Use
Language	English

This Policy establishes the minimum controls required to protect the confidentiality, integrity, availability and traceability of information under the responsibility of GWS. The company handles technical, commercial, contractual and strategic documents related to sensitive institutional relationships, diligences and commercial mandates and therefore requires information discipline consistent with that context and with the criticality of the data handled.

01

PURPOSE

To define basic rules for the use, storage, sharing, protection and disposal of GWS information and documents, as well as those of its clients, partners and counterparties.

02

APPLICABILITY

This Policy applies to:

- partners and officers;
- employees and interns;
- consultants and representatives;
- third parties authorized to access GWS information or environments;
- physical and digital documents held by the company.

03

SECURITY PRINCIPLES

GWS information shall be handled according to the following principles:

- confidentiality: access only by those who need to know;
- integrity: preservation of accuracy and consistency;
- availability: appropriate access when needed;
- traceability: ability to identify use, versions and relevant flows;
- proportionality: controls compatible with the level of sensitivity.

04

INFORMATION CLASSIFICATION

Information shall be classified in a simple and objective way:

Class	Expected use
Public	May be disclosed without relevant risk
Internal	Restricted to the GWS working environment
Confidential	Controlled access, with relevant impact in case of improper disclosure
Restricted	Limited access and enhanced control

Client documents, diligences, non-public opportunities, contracts, technical studies and project environments shall, as a rule, be treated at least as confidential.

05

ACCESS CONTROL

Access to information and systems shall follow the principle of least privilege.

This means that:

- each person receives only the access required for their role;
- credentials are personal and non-transferable;
- access shall be reviewed when there is a change of role, project or termination;
- restricted information requires enhanced control.

Those responsible for an environment, folder, system or project shall ensure that granted access remains consistent with actual functional need.

06

INTERNAL AND EXTERNAL SHARING

All information flow shall observe need, appropriateness and suitable channel.

The following are not allowed:

- sharing confidential documents without a functional basis;
- sending sensitive files through inappropriate channels;
- storing relevant documents in unauthorized environments;
- keeping unnecessary copies of restricted information.

Whenever confidential or restricted information is shared externally, there shall be a legitimate functional basis, minimum recipient control and preference for environments with manageable permissions.

07

CLIENT ENVIRONMENTS AND RESTRICTED DOCUMENTS

Client documents and restricted environments shall, whenever possible, include:

- enhanced authentication;
- permission control by user or project;
- version tracking;
- audit trail for relevant access;
- expiration or periodic review of access.

08

PASSWORDS, MFA AND DEVICES

All persons shall adopt minimum precautions regarding credentials and devices used in GWS activities.

Minimum rules:

- strong, non-shared passwords;
- MFA activation whenever available for critical environments;
- screen lock and basic device protection;
- responsible use of personal devices in professional context.

For remote access, shared networks or use of personal devices, the user shall adopt enhanced caution to avoid improper viewing, unauthorized capture or continued retention of files outside a controlled environment.

09

BACKUP, RETENTION AND DISPOSAL

Relevant information shall follow reasonable retention, recovery and disposal criteria.

Whenever applicable:

- active documents shall remain in a controlled environment;
- obsolete or duplicated files shall be securely removed;
- sensitive materials shall not remain indefinitely without need;
- disposal shall consider the information classification.

10

SECURITY INCIDENTS

Incidents or suspected incidents shall be reported immediately.

Examples include:

- improper sending of a document;
- unauthorized access;
- loss of a device containing GWS information;
- data leak or suspected leak;
- improper alteration of a relevant file.

Every occurrence shall be recorded and handled in proportion to its criticality.

Whenever applicable, the incident response shall include initial containment, preservation of evidence, impact assessment, communication to responsible parties and definition of corrective measures.

11

USER RESPONSIBILITIES

Every person with access to GWS information shall:

- observe the classification applicable to the document or environment;
- maintain minimum organization of folders, versions and naming conventions;
- report improper access, perceived weaknesses or relevant doubts;
- close or return access rights, files and materials when the need for use ceases.

12

TRAINING AND ACCOUNTABILITY

Persons subject to this Policy shall receive adequate guidance on the treatment of information in their work context.

Failure to comply with this Policy may lead to corrective, restrictive, disciplinary or contractual action, depending on the severity of the case.

13

EFFECTIVENESS AND REVIEW

This Policy becomes effective on the date of approval and shall be reviewed periodically or whenever there is a material change in the operational, technological or regulatory environment of GWS.

For internal and institutional GWS use. Document subject to periodic review.

GWS

Connecting Brazil to the World, with governance that earns trust.

www.gwscons.com gws@gwscons.com